

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2001年6月14日 (14.06.2001)

PCT

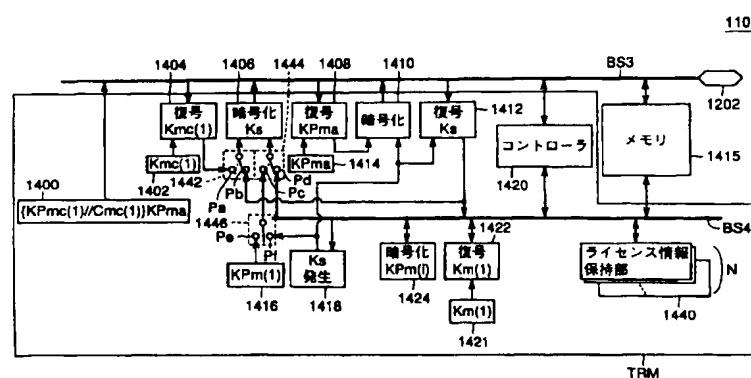
(10) 国際公開番号
WO 01/43342 A1

- (51) 国際特許分類⁷: H04L 9/32, G06F 12/14, G10K 15/02, G06F 13/00
- (21) 国際出願番号: PCT/JP00/08593
- (22) 国際出願日: 2000年12月5日 (05.12.2000)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願平11/346861 1999年12月6日 (06.12.1999) JP
- (71) 出願人(米国を除く全ての指定国について): 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 Osaka (JP). 株式会社 ピーエフュ (PFU LIMITED) [JP/JP]; 〒929-1125 石川県河北郡宇ノ気町宇野気又98番地の2 Ishikawa (JP). 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP). 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP). 日本コロムビア株式会社 (NIPPON COLUMBIA CO., LTD.) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 Tokyo (JP).
- (72) 発明者; および
(75) 発明者/出願人(米国についてのみ): 堀 吉宏 (HORI, Yoshihiro) [JP/JP]. 日置敏昭 (HIOKI, Toshiaki) [JP/JP]. 金森美和 (KANAMORI, Miwa) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内 Osaka (JP). 高橋政孝 (TAKAHASHI, Masatake) [JP/JP]; 〒929-1125 石川県河北郡宇ノ気町宇野気又98番地の2 株式会社 ピーエフュ (PFU LIMITED) [JP/JP]. 長谷部高行 (HASEBE, Takayuki) [JP/JP]. 吉岡 誠 (YOSHIOKA, Makoto) [JP/JP]. 畠山卓久 (HATAKEYAMA, Takahisa) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 利根川忠明 (TONEGAWA, Tadaaki) [JP/JP]; 〒187-8588 東京都小平市上水本町五丁目20番1号 株式会社 日立製作所 半導体グループ内 Tokyo (JP). 穴澤健明 (ANAZAWA, Takeaki) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 日本コロムビア株式会社内 Tokyo (P).
- (74) 代理人: 深見久郎, 外 (FUKAMI, Hisao et al.) ; 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル Osaka (JP).
- (81) 指定国(国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU,

/統葉有

(54) Title: DATA DISTRIBUTION SYSTEM AND RECORDER FOR USE THEREIN

(54) 発明の名称: データ配信システムおよびそれに使用される記録装置



| | |
|--------------------------|------------------------------------|
| 1404...DECRYPTION Km(1) | 1420...CONTROLLER |
| 1406...ENCRYPTION Ks | 1415...MEMORY |
| 1408...DECRYPTION Kpm(0) | 1418...Ks GENERATION |
| 1410...ENCRYPTION | 1424...ENCRYPTION Kpm(1) |
| 1412...DECRYPTION Km(0) | 1422...DECRYPTION Km(1) |
| | 1440...LICENSE INFORMATION HOLDING |

(57) Abstract: A memory card (110) stores access limit information (AC1) in a license information holding section (1440) in a TRM area. The access limit information (AC1) includes information concerning the number of possible reproductions and the number of possessed licenses. A controller (1420) confirms the access limit information (AC1), reproduces and transfers a content, updates it as necessary, and stores the updated access limit information (AC1) in the license information holding section (1440).

/統葉有

WO 01/43342 A1



LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL,
PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ,
UA, UG, US, UZ, VN, YU, ZA, ZW.

- (84) 指定国(広域): ARIPO 特許 (GH, GM, KE, LS, MW,
MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM,
AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許
(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT,
LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG,
CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 國際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイドスノート」を参照。

(57) 要約:

メモリカード (110) は、TRM領域内のライセンス情報保持部 (1440) にアクセス制限情報 (AC1) を格納する。アクセス制限情報 (AC1) は、再生可能回数および所有ライセンス数等の情報を有する。コントローラ (1420) は、コンテンツの再生および移動動作時においては、アクセス制限情報 (AC1) を確認した上で、再生および移動を実行し、実行後は必要に応じて、アクセス制限情報 (AC1) を更新してライセンス情報保持部 (1440) に格納する。

明細書

データ配信システムおよびそれに使用される記録装置

5 技術分野

本発明は、携帯電話機等の端末に対して情報を配信するためのデータ配信システムに関し、より特定的には、コピーされた情報に対する著作権保護を可能とするデータ配信システムおよび当該システムで使用されるメモリカードに関するものである。

10

背景技術

近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

15

このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

20

したがって、このような情報通信網上において音楽データや画像データ等の著作者の権利が存在するコンテンツデータが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

25

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、コンテンツデータの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したCD（コンパクトディスク）については、CDから光磁気ディス

ク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

5 しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化のほとんどないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽データをコピーすることは、著作権保護のために機器の構成上できないようになっている。

10 このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

この場合、情報通信網を通じて公衆に送信されるコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

15

発明の開示

この発明の目的は、情報通信網、たとえば携帯電話機等の情報通信網を介してコンテンツデータを配信することが可能なデータ配信システムおよび当該データ配信システムで使用される記録装置、詳しくはメモリカードを提供することである。

この発明の他の目的は、配信されたコンテンツデータが、著作権者の許可なく複製されることを防止することが可能なデータ配信システムおよび当該データ配信システムで使用される記録装置、詳しくはメモリカードを提供することである。

この発明に従うデータ配信システムは、複数の端末と、コンテンツ供給装置とを備える。コンテンツ供給装置は、外部との間でデータを授受するための第1のインターフェース部と、配信が要求された場合において、アクセス制限情報を生成して、少なくともライセンスキーを含む再生情報とアクセス制限情報を第1のインターフェース部を介して出力するための配信制御部とを含む。各端末は、外部との間でデータを授受するための第2のインターフェース部と、第2のインターフェ

ース部を介して、暗号化コンテンツデータと再生情報とアクセス制限情報を受けて記録する配信データ解読部とを含む。配信データ解読部は、暗号化コンテンツデータ、再生情報およびアクセス制限情報を記録するための記憶部と、外部から再生情報の出力が指示された場合に、記憶部に記録されたアクセス制限情報に基づいて出力の可否を判断する制御部とを有する。

好ましくは、各端末は、コンテンツ再生部をさらに含み、コンテンツ再生部は、外部からコンテンツデータの再生動作が指示された場合において、配信データ解読部から再生情報および暗号化コンテンツデータを受けて、ライセンスキーによって暗号化コンテンツデータを復号して再生するコンテンツデータ再生部を有する。アクセス制限情報は、配信データ解読部からコンテンツ再生部への、再生情報の出力回数を制限する再生制御情報を含む。制御部は、再生動作が指示された場合において、再生制御情報に基づいて再生情報の出力の可否を判断し、再生情報の出力後に必要に応じて再生制御情報を更新する。

好ましくは、アクセス制限情報は、配信データ解読部から他の配信データ解読部に対しての、再生情報の複製可能回数を制限する複製制限情報を含む。制御部は、他の配信データ解読部に対して再生情報を複製する複製動作が外部から指示された場合において、複製制限情報に基づいて再生情報の出力の可否を判断し、再生情報の出力後において、必要に応じて所有ライセンス数情報を更新可能である。

このようなデータ配信システムにおいては、再生可能回数や所有ライセンス数に関するアクセス制限情報を、配信サーバを介さずに、配信データ解読部、より詳しくはメモリカードの内部において、保持および更新できる。したがって、ファイルシステムやアプリケーションプログラム等によって上位レベルからアクセス制限情報を改ざんすることができない構成とすることができます。この結果、再生情報として再生回路の制限付き再生権の発行が可能となり、試聴用としての音楽データ（コンテンツデータ）の配布、安価な再生回数制限付き販売等が、さらには、複数の再生権の配信によって集団購入等のサービスが提供できるようになり、利用者にとって利便性の高いデータ配信システムを提供できるとともに、著作権の保護に対して十分なセキュリティ強度を確保できるため、著作権者の権

利をも守ることができるようになる。

この発明の別の局面に従うと、記録装置は、インターフェース部と、記憶部と、制御部とを備える。インターフェース部は、外部との間でデータを授受する。記憶部は、インターフェース部を介して入力される、格納データおよび格納データの記録装置からの出力を制御するためのアクセス制限情報（AC1）を記録する。制御部は、外部から格納データの出力が指示された場合に、アクセス制限情報に基づいて出力の可否を判断する。

好ましくは、アクセス制限情報は、記録装置から他の機器への格納データの出力回数を制限する出力回数制御情報を含み、制御部は、他の機器に対する格納データの出力が指示された場合において、出力回数制御情報に基づいて出力の可否を判断するとともに、出力後に必要に応じて出力回数制御情報を更新可能である。

好ましくは、アクセス制限情報は、他の記録装置に対する格納データの複製可能な回数を制限する複製制限情報を含み、制御部は、他の記録装置に対する格納データの複製指示が外部から指示された場合において、所有ライセンス数情報に基づいて格納データの出力の可否を判断し、出力後において、必要に応じて複製制限情報を更新可能である。

このような記録装置においては、複製制限情報および出力回数制御情報といったアクセス制限情報を、配信サーバを介さずに記憶領域内部で保持および更新することができる。したがって、ファイルシステムやアプリケーションプログラム等によって上位レベルからアクセス制限情報を改ざんすることができない構成とすることができる。この結果、再生回路の制限付き再生権の発行が可能となり、試聴用としての音楽データ（コンテンツデータ）の配布、安価な再生回数制限付き販売等が、さらには、複数の再生権の配信によって集団購入等のサービスが提供できるようになり、利用者にとって利便性の高いデータ配信システムを提供できるとともに、著作権の保護に対して十分なセキュリティ強度を確保できるため、著作権者の権利をも守ることができるようになる。

図面の簡単な説明

図1は、本発明のデータ配信システムの全体構成を概略的に説明するための概

念図である。

図2は、実施の形態1に従うデータ配信システムにおいて使用される通信のためのデータ、情報等の特性を説明する図である。

図3は、実施の形態1に従うデータ配信システムにおいて使用される鍵データ等の特性をまとめて説明する図である。
5

図4は、図1に示されたライセンスサーバの構成を示す概略ブロック図である。

図5は、図1に示された携帯電話機の構成を示す概略ブロック図である。

図6は、図5に示されたメモリカードの構成を示す概略ブロック図である。

図7は、ライセンス情報保持部に格納される情報の構成を説明する概念図である。
10

図8は、アクセス制限情報AC1の内容を説明する図である。

図9は、実施の形態1に従うデータ配信システムにおける配信セッション時の動作を説明するための第1のフローチャートである。

図10は、実施の形態1に従うデータ配信システムにおける配信セッション時の動作を説明するための第2のフローチャートである。
15

図11は、実施の形態1に従う再生セッション時の動作を説明するためのフローチャートである。

図12は、実施の形態1に従う2つのメモリカード間の複製セッション時の動作を説明するための第1のフローチャートである。

図13は、実施の形態1に従う2つのメモリカード間の複製セッション時の動作を説明するための第2のフローチャートである。
20

図14は、実施の形態1に従う2つのメモリカード間の複製セッション時の動作を説明するための第3のフローチャートである。

図15は、実施の形態2に従うライセンスサーバの構成を示す概略ブロック図である。
25

図16は、実施の形態2に従う携帯電話機の構成を示す概略ブロック図である。

図17は、実施の形態2に従うデータ配信システムにおける配信動作を説明するためのフローチャートである。

図18は、実施の形態2に従う再生動作を説明するフローチャートである。

図1 9は、実施の形態2に従うデータ配信システムにおける2つのメモリカード間の複製セッション時の動作を説明するための第1のフローチャートである。

図2 0は、実施の形態2に従うデータ配信システムにおける2つのメモリカード間における複製セッション時の動作を説明する第2のフローチャートである。

5 図2 1は、実施の形態3に従うメモリカードの構成を示す概略ブロック図である。

図2 2は、再生情報保持部およびライセンス情報保持部に格納される情報の構成を説明する概念図である。

10 発明を実施するための最良の形態

以下、この発明の実施の形態によるデータ配信システムおよび記録装置を図面を参照して詳しく説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

15 なお、以下では携帯電話網を介してデジタル音楽データを各携帯電話ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他のコンテンツデータ、たとえば画像データ、映像データ、教材データ、テキストデータ、朗読（音声）データ、ゲームプログラム等のコンテンツデータを、他の情報通信網を介して配信する場合にも適用することが可能なものである。

20 （実施の形態1）

図1を参照して、著作権の存在する音楽情報を管理するライセンスサーバ10は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア20である携帯電話会社に、このような暗号化コンテンツデータを与える。一方、認証サーバ12は、音楽データの配信を求めてアクセスしてきた携帯電話ユーザの携帯電話機およびメモリカードが正規の機器であるか否かの認証を行なう。

配信キャリア20は、自己の携帯電話網を通じて、各携帯電話ユーザからの配信要求（配信リクエスト）をライセンスサーバ10に中継する。ライセンスサーバ10は、配信リクエストがあると、認証サーバ12により携帯電話ユーザの携

帶電話機およびメモリカード等が正規の機器であることを確認し、要求されたコンテンツデータをさらに暗号化した上で配信キャリア20の携帯電話網を介して、各携帯電話ユーザの携帯電話機に対してコンテンツデータを配信する。

図1においては、たとえば携帯電話ユーザ1の携帯電話機100には、着脱可能なメモリカード110が装着される構成となっている。メモリカード110は、携帯電話機100により受信された暗号化コンテンツデータを受取って、上記配信にあたって行なわれた暗号化については復号した上で、携帯電話機100中の音楽再生部（図示せず）に与える。

さらに、たとえば携帯電話ユーザ1は、携帯電話機100に接続したヘッドホン130等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

以下では、このようなライセンスサーバ10と認証サーバ12と配信キャリア20と併せて、配信サーバ30と総称することにする。

また、このような配信サーバ30から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

このような構成とすることで、まず、メモリカード110を利用しないと、配信サーバ30からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

しかも、このようなコンテンツデータの配信は、携帯電話機網というクローズなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

このとき、たとえばメモリカード112を有する携帯電話ユーザ2が自己の携帯電話機102により、配信サーバ30から直接コンテンツデータの配信を受けることは可能である。しかしながら、相当量の情報量を有するコンテンツデータ

等を携帯電話ユーザ 2 が直接配信サーバ 30 から受信することとすると、この受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該コンテンツデータの配信を受けている携帯電話ユーザ 1 から、そのコンテンツデータをコピーできることを可能としておけば、携帯電話ユーザにとっての利便性が向上する。

図 1 に示すように、携帯電話ユーザ 1 が受信したコンテンツデータを、コンテンツデータそのものおよび当該コンテンツデータを再生可能するために必要な情報とともに、携帯電話ユーザ 2 に対してコピーさせる場合をコンテンツデータの「複製」と呼ぶ。

この場合に、携帯電話機 100 および 102 を介して、メモリカード 110 と 112との間で暗号化されたコンテンツデータ（音楽データ）および再生のために必要な情報（再生情報）が複製される。ここで、「再生情報」とは、後に説明するように、所定の暗号化方式に従って暗号化されたコンテンツデータを復号可能なライセンスキーと、著作権保護にかかわる情報であるライセンス ID やアクセス再生に関する制限情報等とを有する。

このような構成とすることによって、一旦配信サーバ 30 より配信を受けたコンテンツデータについて受信者側での柔軟な利用が可能となる。

また、携帯電話機 100 および 102 が PHS (Personal Handy Phone) である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、携帯電話ユーザ 1 と携帯電話ユーザ 2 との間における情報の複製を行なうことが可能である。

図 1 に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話ユーザ側で再生可能するためにシステム上必要とされるのは、第 1 には、通信における暗号鍵を配信するための方式であり、さらに第 2 には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第 3 には、このように配信されたコンテンツデータの無断コピーを防止するための復号鍵保護を実現する構成である。

本発明の実施の形態においては、特に、配信、再生および複製の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチエ

ック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびコンテンツ再生回路（携帯電話機）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。また、再生回数の制限を設けた再生権の発行を可能とし、利用者にとって利便性が高く、かつ著作権に対して十分なセキュリティー強度を維持できる構成を説明する。

次に図2を用いて、図1に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する。

まず、配信サーバより配信されるデータについて説明する。Data は、音楽データ等のコンテンツデータである。コンテンツデータ Data には、ライセンスキー Kc で復号可能な暗号化が施される。ライセンスキー Kc によって復号可能な暗号化が施された暗号化コンテンツデータ {Data} Kc がこの形式で配信サーバ 30 より携帯電話ユーザに配布される。

なお、以下においては、{Y} X という表記は、データ Y を、復号鍵 X により復号可能な暗号化を施したデータであることを示すものとする。

さらに、配信サーバからは、暗号化コンテンツデータとともに、コンテンツデータに関するあるいはサーバへのアクセスに関する平文情報としての付加情報 Data-inf が配布される。また、ライセンスとしては、コンテンツデータ Data を識別するためのコードであるコンテンツ ID およびライセンスの発行を特定できる管理コードであるライセンス ID や、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件 AC に基づいて生成される、メモリのアクセスに対する制限に関する情報であるアクセス制限情報 AC 1 および再生回路における制御情報である再生回路制御情報 AC 2 等が存在する。

後ほど詳細に説明するが、再生回路制御情報 AC 2 は、再生回数の制限や複製（移動）可能なライセンス数を示す情報を含み、メモリカード内において情報の管理および更新が実行される。

図3には、図1に示したデータ配信システムにおいて使用されるキーデータ（鍵データ）等の特性が示される。

図3を参照して、コンテンツ再生回路（携帯電話機）およびメモリカードには

固有の公開暗号鍵 KPp (n) および KPmc (m) がそれぞれ設けられ、公開暗号鍵 KPp (n) および KPmc (m) はコンテンツ再生回路（携帯電話機）のクラス固有の秘密復号鍵 Kp (n) およびメモリカードのクラス固有の秘密復号鍵 Kmc (m) によってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、携帯電話機の種類ごとおよびメモリカードのクラスごとに異なる値を持つ。

また、メモリカードおよび再生回路のクラス証明書として、Cp (n) および Cmc (m) がそれぞれ設けられる。ここで、自然数 m はメモリカードの、自然数 n はコンテンツ再生回路（携帯電話機）のクラスを区別するための番号を表わす。

これらのメモリカードおよびコンテンツ再生部固有の公開暗号鍵およびクラス証明書は、{KPmc (m) //Cmc (m)} KPma および {KPp (n) //Cp (n)} KPma の形式で、出荷時にメモリカードおよび携帯電話機にそれぞれ記録される。後ほど詳細に説明するが、KPma は配信システム全体で共通の認証鍵である。認証鍵 KPma を用いて認証データを復号すると、その復号結果から認証データの正当性が確認できる。言い換えれば、認証鍵 KPma は、クラス固有の公開暗号鍵およびその証明書であるクラス証明書を承認するために用いられる鍵である。なお、認証データを作成するための暗号化は、認証鍵と対をなす非対称な秘密鍵によって行なわれる。

メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、再生および複製が行なわれるごとにサーバ 30、携帯電話機 100 または 102、メモリカード 110 または 112において生成される共通鍵 Ks 1 ~ Ks 4 が用いられる。

ここで、共通鍵 Ks 1 ~ Ks 4 は、サーバ、携帯電話機もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵 Ks 1 ~ Ks 4 を「セッションキー」とも呼ぶこととする。

これらのセッションキー Ks 1 ~ Ks 4 は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモリカードによって管理される。具体的には、セッションキー Ks 1 は、配信サーバによって配信セッションごとに発生される。セッションキー Ks 2 は、メモリカードによって配信セッション

および複製（受信側）セッションごとに発生し、セッションキーK_s3は、同様にメモリカードにおいて再生セッションおよび複製（送信側）セッションごとに発生する。セッションキーK_s4は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンスキー等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。
5

また、メモリカード100内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される暗号鍵K_{Pm}(i) (i:自然数)と、暗号鍵K_{Pm}(i)で暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵K_m(i)が存在する。ここで、自然数iは、各メモリカードを区別するための番号を表わす。
10

その他の鍵としては、再生回路に共通の秘密鍵として、主としてライセンスキーK_cの取得に利用される共通鍵方式における秘密鍵K_{com}が存在する。秘密鍵K_{com}は、配信サーバおよび携帯電話機の双方において保持され、ライセンスキーK_c等の暗号化および取得のための復号処理にそれぞれ使用される。
15

なお、共通鍵K_{com}を、公開鍵方式における公開暗号鍵K_{Pcom}および秘密復号鍵K_{com}の組に置き換えて運用することも可能である。この場合には、公開暗号鍵K_{Pcom}は配信サーバに保持されてライセンスキーK_cの暗号化に使用され、秘密復号鍵K_{com}は、携帯電話機に保持されてライセンスキーK_cの取得に使用される。
20

図4を参照して、ライセンスサーバ10は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンスID等の配信情報を保持するための情報データベース304と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース302と、情報データベース304および課金データベース302からのデータをデータバスBS1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。
25

データ処理部 310 は、データバス BS1 上のデータに応じて、データ処理部 310 の動作を制御するための配信制御部 315 と、配信制御部 315 に制御されて、配信セッション時にセッションキー K_{s1} を発生するためのセッションキー発生部 316 と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ $\{K_{Pmc}(m) // C_{mc}(m)\} K_{Pma}$ および $\{K_{Pp}(n) // C_p(n)\} K_{Pma}$ を通信装置 350 およびデータバス BS1 を介して受けて、認証鍵 K_{Pma} による復号処理を行なう復号処理部 312 とを含む。
5

データ処理部 310 は、さらに、セッションキー発生部 316 より生成されたセッションキー K_{s1} を復号処理部 312 によって得られた公開暗号鍵 $K_{Pmc}(m)$ 10 を用いて暗号化して、データバス BS1 に出力するための暗号化処理部 318 と、セッションキー K_{s1} によって暗号化された上で送信されたデータをデータバス BS1 をより受けて、復号処理を行なう復号処理部 320 と、再生回路に共通な秘密鍵 K_{com} を保持する K_{com} 保持部 322 とを含む。

データ処理部 310 は、さらに、配信制御部 315 から与えられるライセンスキー K_c および再生回路制御情報 AC2 を再生回路共通の秘密鍵 K_{com} で暗号化する暗号化処理部 324 と、暗号化処理部 324 から出力されたデータを復号処理部 320 によって得られたメモリカード固有の公開暗号鍵 $K_{Pm}(i)$ によって暗号化するための暗号化処理部 326 と、暗号化処理部 326 の出力を、復号処理部 320 から与えられるセッションキー K_{s2} によってさらに暗号化してデータバス BS1 に出力するための暗号化処理部 328 とを含む。
15
20

なお、共通鍵方式における秘密復号 K_{com} に代えて、公開鍵方式における公開暗号鍵 K_{Pcom} および秘密復号鍵 K_{com} の組を用いる場合には、 K_{com} 保持部 322 に相当する部分に公開暗号鍵 K_{Pcom} が保持される。さらに、暗号化処理部 324 によって、公開暗号鍵 K_{Pcom} による暗号化が行なわれる。

25 ライセンスサーバ 10 の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

図 5 を参照して、携帯電話機 100においては、携帯電話機のクラスを表わす自然数 $n = 1$ 、携帯電話機を個別に識別する自然数 $i = 1$ とする。

携帯電話機 100 は、携帯電話網により無線伝送される信号を受信するための

アンテナ 1102 と、アンテナ 1102 からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ 1102 に与えるための送受信部 1104 と、携帯電話機 100 の各部のデータ授受を行なうためのデータバス BS2 と、データバス BS2 を介して携帯電話機 100 の動作を制御するためのコントローラ 1106 とを含む。

携帯電話機 100 は、さらに、外部からの指示を携帯電話機 100 に与えるためのタッチキー部 1108 と、コントローラ 1106 等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ 1110 と、通常の通話動作において、データベース BS2 を介して与えられる受信データに基づいて音声を再生するための音声再生部 1112 と、外部との間でデータの授受を行なうためのコネクタ 1120 と、コネクタ 1120 からのデータをデータバス BS2 に与え得る信号に変換し、または、データバス BS2 からのデータをコネクタ 1120 に与え得る信号に変換するための外部インターフェース部 1122 とを含む。

携帯電話機 100 は、さらに、配信サーバ 30 からのコンテンツデータ（音楽データ）を記憶しつつ復号化処理するための着脱可能なメモリカード 110 と、メモリカード 110 とデータバス BS2 との間のデータの授受を制御するためのメモリインターフェース 1200 と、携帯電話機のクラスごとにそれぞれ設定される公開暗号鍵 K_{Pp} (1) およびクラス証明書 C_p (1) を公開復号鍵 K_{Pm a} で復号可能な状態に暗号化したデータを保持する認証データ保持部 1500 を含む。

携帯電話機 100 は、さらに、携帯電話機（コンテンツ再生回路）固有の復号鍵である K_p (1) を保持する K_p 保持部 1502 と、データバス BS2 から受けたデータを K_p (1) によって復号しメモリカードによって発生されたセッションキー K_{s 3} を得る復号処理部 1504 と、メモリカード 110 に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード 110 との間でデータバス BS2 上においてやり取りされるデータを暗号化するためのセッションキー K_{s 4} を乱数等により発生するセッションキー発生部 1508 と、生成されたセッションキー K_{s 4} を復号処理部 1504 によって得られたセッションキー K_{s 3} によって暗号化しデータバス BS2 に出力する暗号化処理部 1506 と、デー

タバス BS 2 上のデータをセッションキー K_s 4 によって復号して出力する復号処理部 1510 とを含む。

携帯電話機 100 は、さらに、再生回路に共通に設定される秘密鍵 K_{com} を保持する K_{com} 保持部 1512 と、復号処理部 1510 が output する $\{K_c//AC\}$ 5 K_{com} を秘密鍵 K_{com} で復号しライセンスキー K_c および再生回路制御情報 AC 2 を出力する復号処理部 1514 と、データバス BS 2 より暗号化コンテンツデータ $\{Data\}$ K_c を受けて、復号処理部 1514 より取得してライセンスキー K_c によって復号しコンテンツデータを出力する復号処理部 1516 とを含む。携帯電話機 100 は、さらに、復号処理部 1516 の出力を受けてコンテンツデータを再生するための音楽再生部 1518 と、音楽再生部 1518 と音声再生部 1112 10 の出力を受けて、動作モードに応じて選択的に出力するための切換部 1525 と、切換部 1525 の出力を受けて、ヘッドホン 130 と接続するための接続端子 1530 とを含む。

なお、共通鍵 K_{com} に代えて公開鍵方式における公開暗号鍵 K_{Pcom} および秘密復号鍵 K_{com} の組を用いる場合には、 K_{com} 保持部 1512 に相当する部分に秘密復号鍵 K_{com} が保持される。さらに、復号処理部 1514 によって、秘密復号鍵 K_{com} による復号が行なわれる。

また、図 5においては、説明の簡素化のため、携帯電話機のうち本発明のコンテンツデータの配信および再生にかかるblockのみを記載し、携帯電話機が 20 本来備えている通話機能に関するblockについては一部割愛している。

図 5に記載されたblockのうち、アンテナ 1102、送受信部 1104、コントローラ 1106、キー 1108、ディスプレイ 1110、音声再生部 1112、コネクタ 1120、外部インターフェース 1122、切換部 1525 および接続端子 1530 の、通話処理に関するあるいは通話処理と共にされるblock群 25 除いた部分が、コンテンツデータの配信および再生に関するコンテンツ再生部に相当する。なお、携帯電話ユーザの利便性を図るために、携帯電話機 100 のうちのコンテンツ再生部に相当するblock群を、音楽再生モジュールとして着脱可能なモジュール化する構成を採用することも可能である。

携帯電話機 100 の各構成部分の各セッションにおける動作については、後ほ

どフローチャートを使用して詳細に説明する。

図6を参照して、既に説明したように、公開暗号鍵 $KP_m(i)$ およびこれに対応する秘密復号鍵 $K_m(i)$ は、メモリカードごとに固有の値であるが、メモリカード110においては、この自然数 $i=1$ として取扱う。また、メモリカードの固有の公開暗号鍵および秘密復号鍵として、 $KP_{mc}(m)$ および $K_{mc}(m)$ が設けられ、メモリカードのクラス証明書として $C_{mc}(m)$ が設けられるが、メモリカード110においては、これらは自然数 $m=1$ でそれぞれ表わされるものとする。

メモリカード110は、認証データ $\{KP_{mc}(1) // C_{mc}(1)\}$ KP_{ma} を保持する認証データ保持部1400と、メモリカードの種類ごとに設定される固有の復号鍵である $K_{mc}(1)$ を保持する K_{mc} 保持部1402と、メモリカードごとに固有に設定される秘密復号鍵 $K_m(1)$ を保持する $K_m(1)$ 保持部1421と、 $K_m(1)$ によって復号可能な公開暗号鍵 $KP_m(1)$ を保持する $KP_m(1)$ 保持部1416とを含む。認証データ保持部1400は、メモリカード110に対応して設定される公開暗号鍵 $KP_{mc}(1)$ を認証鍵 KP_{ma} で復号することで認証可能な状態に暗号化して保持する。

このように、メモリカードという記録装置の公開暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンスキーの管理をメモリカード単位で実行することが可能になる。

メモリカード110は、さらに、メモリインターフェース1200との間で信号を端子1202を介して授受するデータバスBS3と、データバスBS3にメモリインターフェース1200から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵 $K_{mc}(1)$ を $K_{mc}(1)$ 保持部1402から受けて配信サーバ30が配信セッションにおいて生成したセッションキーKs1、または他のメモリカードが複製セッションにおいて生成したセッションキーKs3を接点Paに出力する復号処理部1404とを含む。

メモリカード110は、さらに、 KP_{ma} 保持部1414から認証鍵 KP_{ma} を受け、データバスBS3に与えられるデータから認証鍵 KP_{ma} による復号処理を実行して復号結果を暗号化処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1444

によって選択的に与えられるデータを暗号化してデータバス BS 3 に出力する暗号化処理部 1406 を含む。

メモリカード 110 は、さらに、配信、再生および複製の各セッションにおいてセッションキーを発生するセッションキー発生部 1418 と、セッションキー発生部 1418 の出力したセッションキー $K_s 3$ を復号処理部 1408 によって得られる公開暗号鍵 $K_{Pp} (n)$ もしくは $K_{Pmc} (m)$ によって暗号化してデータバス BS 3 に送出する暗号化処理部 1410 と、BS 3 よりセッションキー $K_s 3$ によって暗号化されたデータを受けてセッションキー発生部 1418 より得たセッションキー $K_s 3$ によって復号し、復号結果をデータバス BS 4 に送出する復号処理部 1412 を含む。
10

メモリカード 110 は、さらに、「複製」時にデータバス BS 4 上のデータを他のメモリカードの公開暗号鍵 $K_{Pm} (i)$ ($i \neq 1$) で暗号化する暗号化処理部 1424 と、データバス BS 4 上のデータを公開暗号鍵 $K_{Pm} (1)$ と対をなすメモリカード 110 固有の秘密復号鍵 $K_m (1)$ によって復号するための復号処理部 1422 と、公開暗号鍵 $K_{Pm} (1)$ で暗号化されている、ライセンスキー K_c および再生回路制御情報 AC_2 をデータバス BS 4 より受けて格納するとともに、暗号化コンテンツデータ {Data} K_c および付加情報 $Data-inf$ をデータバス BS 3 より受けて格納するためのメモリ 1415 を含む。
15

メモリカード 110 は、さらに、復号処理部 1422 によって得られるライセンス ID、コンテンツ ID およびアクセス制限情報 AC_1 を保持するためのライセンス情報保持部 1440 と、データバス BS 3 を介して外部との間でデータ授受を行ない、データバス BS 4 との間で再生情報等を受けて、メモリカード 110 の動作を制御するためのコントローラ 1420 を含む。ライセンス情報保持部 1440 は、データバス BS 4 との間でライセンス ID、コンテンツ ID およびアクセス制限情報 AC_1 のデータの授受が可能である。
20
25

図 7 を参照して、ライセンス情報保持部 1440 は、N 個 (N : 自然数) のバンクを有し、各ライセンスに対応するライセンス情報である、ライセンス ID、データコンテンツ ID データおよびアクセス制限情報 AC_1 をバンクごとに保持する。

図 8 を参照して、アクセス制限情報 AC 1 は、再生回数制限情報 Sub_Play と、所有ライセンス数 Sub_Move とを含む。図 8においては、再生回数制限情報 Sub_Play は、一例として 8 ビットのデータである。Sub_Play の値が FF(h) である場合には再生回数に制限がないことを示し、その値が 0 (h) である場合には、
5 もはや再生不能であることを示す。また、Sub_Play の値が 1 (h) ~ 7F(h) の範囲である場合は、この値は再生可能な回数を示し、再生されるごとに Sub_Play の値は減じられる。なお、(h) は、16 進数表示を意味する。

また、図 8においては、所有ライセンス数 Sub_Move は、一例として同様に 8 ビットのデータで示される。Sub_Move の値が FF(h) である場合には、複製が禁止
10 されていることを示す。また、Sub_Move の値が 0 (h) ~ 7F(h) の範囲である場合は、この値は所有ライセンス数を示し、他のメモリカードに複製させるごとに、複製したライセンス数に応じて Sub_Move の値は減じられ、その値が 0 (h) となっ
た場合には、もはや複製するライセンスが無いことを示す。

15 アクセス制限情報 AC 1 は、ライセンス購入時に利用者側からの指定に応じて生成されるライセンス購入条件 AC に応じて、配信動作時に配信サーバ 30 によって発行され、再生および複製動作が実行されるごとに、メモリカード 110 内において、更新および保持される。

20 なお、図 6において、実線で囲んだ領域は、メモリカード 110 内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュール TRM に組込まれているものとする。このようなモジュールは、一般には、内部解析や改ざんを物理的および論理的に防衛する技術を用いた、外部から直接アクセス不可能なタンパーレジスタントモジュール (Tamper Resistant Module) である。

25 もちろん、メモリ 1415 も含めて、モジュール TRM 内に組込まれる構成としてもよい。しかしながら、図 6 に示したような構成とすることで、メモリ 1415 中に保持されている再生に必要な再生情報は、いずれも暗号化されているデータであるため、第三者はこのメモリ 1415 中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタントモジュール内にメモリ

1415を設ける必要がないので、製造コストが低減されるという利点がある。

次に、本発明の実施の形態に従うデータ配信システムの各セッションにおける動作についてフローチャートを参照して詳しく説明する。

5 まず、図9および図10のフローチャートを用いて、実施の形態1に従うデータ配信システムにおけるコンテンツの購入時に発生する配信セッション時の動作（以下、配信動作ともいう）を説明する。

図9および図10においては、携帯電話ユーザ1が、メモリカード110を用いることで、携帯電話機100を介して配信サーバ30から音楽データであるコンテンツデータの配信を受ける場合の動作が説明される。

10 図9を参照して、まず、携帯電話ユーザ1の携帯電話機100から携帯電話ユーザによりタッチキー部1108のキーボタンの操作等によって、配信リクエストがなされる（ステップS100）。

15 メモリカード110においては、この配信リクエストに応じて、認証データ保持部1400より認証データ {KPmc (1) //Cmc (1) } KPma が出力される（ステップS102）。

携帯電話機100は、メモリカード110から受理した認証のための認証データ {KPmc (1) //Cmc (1) } KPma に加えて、コンテンツ再生回路の認証のための認証データ {KPp (1) //Cp (1) } KPma と、コンテンツID、ライセンス購入条件データACとを配信サーバ30に対して送信する（ステップS104）。

20 配信サーバ30では、携帯電話機100からコンテンツID、認証データ {KPp (1) //Cp (1) } KPma、 {KPmc (1) //Cmc (1) } KPma、 {KPp (1) //Cp (1) } KPma、ライセンス購入条件ACを受信し（ステップS106）、復号処理部312において認証鍵KPmaで復号処理を実行して、メモリカード110の公開暗号鍵およびクラス証明書であるKPmc (1) およびCmc (1) と、携帯電話機100のコンテンツ再生回路の公開暗号鍵およびクラス証明書であるKPp (1) およびCp (1) を受理する（ステップS108）。

25 配信制御部315は、受理したクラス証明データCmc (1) およびCp (1)に基づいて、認証サーバ12に対して照会を行ない、これらのクラス証明書が有効であれば正規の機器であり、これらの公開暗号鍵が有効であることが確認される。

公開暗号鍵が有効である場合には次の処理（ステップS112）に移行し、これらの公開暗号鍵が無効である場合には、処理を終了（ステップS160）する（ステップS110）。

なお、認証データ {KP_{mc} (1)} KP_{ma} および認証データ {KP_p (1)} KP_{ma} は、
5 それぞれが認証鍵 KP_{ma} によって復号することで、その正当性が判断可能な暗号化が施されているため、認証サーバ12 に対して照会を行なわず、ライセンスサーバ10 の配信制御部315 が、認証鍵 KP_{ma} による復号結果から独自に認証を行なう構成とすることもできる。

照会の結果、正規のクラス証明書を持つメモリカードと再生回路とを備える携
10 帯電話機からのアクセスであることが確認されると、配信サーバ30において、セッションキー発生部316 は、配信のためのセッションキーK_{s1} を生成する。セッションキーK_{s1} は、復号処理部312 によって得られたメモリカード110 に対応する公開暗号鍵 KP_{mc} (1) によって、暗号化処理部318 によって暗号化される（ステップS112）。

15 暗号化されたセッションキーK_{s1} は、{K_{s1}} K_{mc} (1) として、データバス BS1 および通信装置350 を介して外部に出力される（ステップS114）。

携帯電話機100 が、暗号化されたセッションキー {K_{s1}} K_{mc} (1) を受信すると（ステップS116）、メモリカード110 においては、メモリインターフェース1200 を介して、データバス BS3 に与えられた受信データを、復号処理部1404 が、保持部1402 に保持されるメモリカード110 固有の秘密復号鍵 K_{mc} (1) により復号処理することにより、セッションキーK_{s1} を復号し抽出する（ステップS118）。

コントローラ1420 は、配信サーバ30 で生成されたセッションキーK_{s1} の受理を確認すると、セッションキー発生部1418 に対して、メモリカードにおいて配信動作時に生成されるセッションキーK_{s2} の生成を指示する。
25

暗号化処理部1406 は、切換スイッチ1442 の接点Pa を介して復号処理部1404 より与えられるセッションキーK_{s1} によって、切換スイッチ1444 および1446 の接点を順次切換えることによって与えられるセッションキーK_{s2} および公開暗号鍵 KP_m (1) を1つのデータ列として暗号化して、{K_{s2}

//KPm (1) } Ks 1 をデータバス BS 3 に出力する (ステップ S 1 2 0)。

データバス BS 3 に出力された暗号データ {Ks 2 //KPm (1) } Ks 1 は、データバス BS 3 から端子 1 2 0 2 およびメモリインターフェース 1 2 0 0 を介して携帯電話機 1 0 0 に送信され、携帯電話機 1 0 0 から配信サーバ 3 0 に送信される
5 (ステップ S 1 2 2)。

配信サーバ 3 0 は、暗号化データ {Ks 2 //KPm (1) } Ks 1 を受信して、復号処理部 3 2 0 においてセッションキー Ks 1 による復号処理を実行し、メモリカード 1 1 0 で生成されたセッションキー KS 2 およびメモリカード 1 1 0 固有の公開暗号鍵 KPm (1) を受理する (ステップ S 1 2 4)。

10 配信制御部 3 1 5 は、ステップ S 1 0 6 で取得したコンテンツ ID およびライセンス購入条件 AC に従って、ライセンス ID、アクセス制限情報 AC 1 および再生回路制御情報 AC 2 を生成する (ステップ S 1 2 6)。さらに、暗号化コンテンツデータを復号するためのライセンスキー Kc を情報データベース 3 0 4 より取得する (ステップ S 1 2 8)。

15 図 1 0 を参照して、配信制御部 3 1 5 は、取得したライセンスキー Kc および再生回路制御情報 AC 2 を暗号化処理部 3 2 4 に与える。暗号化処理部 3 2 4 は、Kcom 保持部 3 2 2 より得られる、再生回路共通の秘密鍵 Kcom によって、ライセンスキー Kc および再生回路制御情報 AC 2 を暗号化する (ステップ S 1 3 0)。

20 暗号化処理部 3 2 4 が output する暗号化データ {Kc//AC 2 } Kcom と、配信制御部 3 1 5 が output するライセンス ID、コンテンツ ID およびアクセス制限情報 AC 1 とは、暗号化処理部 3 2 6 によって、復号処理部 3 2 0 によって得られたメモリカード 1 1 0 固有の公開暗号鍵 KPm (1) によって暗号化される (ステップ S 1 3 2)。暗号化処理部 3 2 8 は、暗号化処理部 3 2 6 の出力を受けて、メモリカード 1 1 0 において生成されたセッションキー Ks 2 によって暗号化する。暗号化処理部 3 2 8 より出力された暗号化データは、データバス BS 1 および通信装置 3 5 0 を介して携帯電話機 1 0 0 に送信される (ステップ S 1 3 4)。

25 このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやりとりし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信において

も事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

携帯電話機 100 は、送信された暗号化データ { { {Kc//AC2} Kcom//ライセンス ID//コンテンツ ID//AC1 } Km (1) } Ks2 を受信し（ステップ S136）、
5 メモリカード 110においては、メモリインターフェース 1200 を介して、データバス BS3 に与えられた受信データを復号化処理部 1412 によって復号する。復号処理部 1412 は、セッションキー発生部 1418 から与えられたセッションキー Ks2 を用いてデータバス BS3 の受信データを復号しデータバス BS4 に出力する（ステップ S138）。

10 この段階で、データバス BS4 には、Km (1) 保持部 1421 に保持される秘密復号鍵 Km (1) で復号可能な { {Kc//AC2} Kcom //ライセンス ID//コンテンツ ID//AC1 } Km (1) が output される。コントローラ 1420 の指示によって、{ {Kc//AC2} Kcom//ライセンス ID//コンテンツ ID//AC1 } Km (1) は、メモリ 1415 に記録される（ステップ S140）。一方、{ {Kc//AC2} Kcom//ライセンス ID//コンテンツ ID//AC1 } Km (1) は、復号処理部 1422 において、
15 秘密復号鍵 Km (1) によって復号され、ライセンス ID、コンテンツ ID およびアクセス制限情報 AC1 のみが受理される（ステップ S142）。

ライセンス ID、コンテンツ ID およびアクセス制限情報 AC1 については、ライセンス情報保持部 1440 に記録される（ステップ S144）。

20 ステップ S144 までの処理がメモリ回路で正常に終了した段階で、携帯電話機 100 から配信サーバ 30 にコンテンツデータの配信要求がなされる（ステップ S146）。

配信サーバ 30 は、コンテンツデータの配信要求を受けて、情報データベース 304 より、暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf を取得して、これらのデータをデータバス BS1 および通信装置 350 を介して出力する（ステップ S148）。

携帯電話機 100 は、{Data} Kc//Data-inf を受信して、暗号化コンテンツデータ {Data} Kc および Data-inf を受理する（ステップ S150）。暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf はメモリインターフェース 1

200および端子1202を介してメモリカード110のデータバスBS3に伝達される。メモリカード110においては、受信した{Data}Kcおよび付加情報Data-infがそのままメモリ1415に記録される(ステップS152)。

さらに、メモリカード110から配信サーバ30へは、配信受理の通知が送信され(ステップS154)、配信サーバ30で配信受理を受信すると(ステップS156)、課金データベース302への課金データの格納等を伴って、配信終了の処理が実行され(ステップS158)、全体の処理が終了する(ステップS160)。

このようにして、携帯電話機100のコンテンツ再生部およびメモリカード110が正規の機器であること、同時に、それぞれがクラス証明書Cp(1)およびCmc(1)とともに暗号化して送信できた公開暗号鍵Kp(1)およびKmc(1)が有効であることを確認した上で、コンテンツデータを配信することができ、十分なセキュリティ強度を確保することができる。

次に、図11のフローチャートを用いて、携帯電話機100内において、メモリカード110に保持された暗号化コンテンツデータから音楽を再生し、外部に出力するための再生セッション時の動作(以下、再生動作ともいう)を説明する。

図11を参照して、携帯電話機100のタッチキーパー1108等からの携帯電話ユーザ1の指示により、再生リクエストが生成される(ステップS200)。携帯電話機100は、再生リクエストの生成に応じて、認証データ保持部150より、認証鍵KPmaで復号することで認証可能な認証データ{KPP(1)//Cp(1)}KPmaをデータバスBS2に出力する(ステップS202)。

認証データ{KPP(1)//Cp(1)}KPmaは、データバスBS2およびメモリインターフェース1200を介してメモリカード110に伝達される。

メモリカード110においては、端子1202を介してデータバスBS3に伝達される認証のための暗号化データ{KPP(1)//Cp(1)}KPmaは、復号処理部1408に取込まれる。復号処理部1408は、KPma保持部1414から認証鍵KPmaを受けて、データバスBS3のデータを復号処理し、コンテンツ再生部すなわち携帯電話機100の種類に固有の公開暗号鍵KPP(1)およびクラス証明書Cp(1)を得る。コントローラ1420は、データバスBS3を介して公開

暗号鍵 K_{Pp} (1) およびクラス証明書 C_p (1) を受理する (ステップ S 204)。

コントローラ 1420 は、復号処理部 1408 の復号結果に基づいて、受理した携帯電話機 100 のコンテンツ再生回路の認証作業を行ない、携帯電話機 100 のコンテンツ再生回路が承認されたものである場合には処理を次のステップ 5 (ステップ S 208) に進める (ステップ S 206)。一方、携帯電話機 100 のコンテンツ再生回路が非承認である場合には、再生セッションの処理を終了する (ステップ S 240)。

次に、コントローラ 1420 は、セッションキー発生部 1418 に、再生セッションにおけるセッションキー K_{s3} の生成をデータバス BS4 を介して指示する。セッションキー発生部 1418 によって生成されたセッションキー K_{s3} は、暗号化処理部 1410 に送られる。暗号化処理部 1410 は、復号処理部 1408 によって得られた携帯電話機 100 の公開暗号鍵 K_{Pp} (1) によってセッションキー K_{s3} を暗号化し K_{Pp} (1) に対応する秘密復号鍵 K_p (1) で復号可能な暗号化データ {K_{s3}} K_p (1) をデータバス BS3 に出力する (ステップ S 208)。

携帯電話機 100 は、端子 1202 およびメモリインターフェース 1200 を介して、データバス BS に暗号化データ {K_{s3}} K_p (1) を受ける。暗号化データ {K_{s3}} K_p (1) は、復号処理部 1504 によって復号され、メモリカード 110 で生成されたセッションキー K_{s3} が受理される (ステップ S 210)。

コントローラ 1106 は、セッションキー K_{s3} の受理に応じて、セッションキー発生部 1508 に対して、再生セッションにおいて携帯電話機 100 で生成されるセッションキー K_{s4} の発生をデータバス BS2 を介して指示する。生成されたセッションキー K_{s4} は暗号化処理部 1506 に送られ、復号処理部 1504 によって得られたセッションキー K_{s3} によって暗号化された {K_{s4}} K_{s3} がデータバス BS2 に受理される (ステップ S 212)。

暗号化されたセッションキー {K_{s4}} K_{s3} は、メモリインターフェース 1200 を介してメモリカード 110 に伝達される。メモリカード 110 においては、データバス BS3 に伝達される暗号化されたセッションキー {K_{s4}} K_{s3} を復号処理部 1412 によって復号し、携帯電話機 100 で生成されたセッションキー K_{s4} を受理する (ステップ S 214)。

セッションキーKs 4 の受理に応じて、コントローラ 1 4 2 0 は、ライセンス情報保持部 1 4 4 0 内の対応するアクセス制限情報 AC 1 を確認する。

コントローラ 1 4 2 0 は、まず所有ライセンス数 Sub_Move を確認し、この値が 0 であるときは、すでにライセンスが無い状態であるので再生セッションを終了する（ステップ S 2 4 0）。一方、所有ライセンス数 Sub_Move の値が 0 以外であるときには、処理を次のステップに進める（ステップ S 2 1 6）。

次のステップにおいては、コントローラ 1 4 2 0 は、再生回数制限情報 Sub_Play を確認し、この値が 0 であるときは、すでに再生不能の状態であるので再生セッションを終了する（ステップ S 2 4 0）。再生回数制限情報 Sub_Play の値が 1 (h)～7F(h) である場合には、Sub_Play の値すなわち再生可能回数を 1 減じて（ステップ S 2 2 0）、再生セッションの処理を進める。一方、再生回数制限情報 Sub_Play の値が FF(h) である場合には、当該ライセンスについては再生回数の制限がないことを意味するので、ステップ S 2 2 0 を実行することなく再生セッションの処理が実行される（ステップ S 2 1 8）。

ステップ S 2 1 8において、当該再生セッションにおいて再生が可能であると判断された場合には、メモリに記録された再生リクエスト曲のライセンスキー Kc および再生回路制御情報 AC 2 の復号処理が実行される。具体的には、コントローラ 1 4 2 0 の指示に応じて、メモリ 1 4 1 5 からデータバス BS 4 に読出された暗号化データ { {Kc//AC 2} Kcom // ライセンス ID // コンテンツ ID // AC 1 } Km (1) を復号処理部 1 4 2 2 がメモリカード 1 1 0 固有の秘密復号鍵 Km (1) によって復号し、共通の秘密鍵 Kcom によって復号可能な暗号化データ {Kc//AC 2} Kcom がデータバス BS 4 上に得られる（ステップ S 2 2 2）。

得られた暗号化データ {Kc//AC 2} Kcom は、切換スイッチ 1 4 4 4 の接点 Pd を介して暗号化処理部 1 4 0 6 に送られる。暗号化処理部 1 4 0 6 は、切換スイッチ 1 4 4 2 の接点 Pb を介して復号処理部 1 4 1 2 より受けたセッションキー Ks 4 によってデータバス BS 4 から受けた暗号化データをさらに暗号化し、{ {Kc//AC 2} Kcom } Ks 4 をデータバス BS 3 に出力する（ステップ S 2 2 4）。

データバス BS 3 に出力された暗号化データは、メモリインターフェース 1 2 0 0 を介して携帯電話機 1 0 0 に送出される。

携帯電話機 100においては、メモリインターフェース 1200を介してデータバス BS2に伝達される暗号化データ { {Kc//AC2} Kcom} Ks4を復号処理部 1510によって復号処理を行ない、暗号化されたライセンスキー Kc および再生回路制御情報 AC2を受理する（ステップ S226）。

5 復号処理部 1514は、暗号化データ { {Kc//AC2} Kcom} を、Kcom 保持部 1512から受けた再生回路に共通の秘密鍵 Kcom によって復号し、ライセンスキー Kc および再生回路制御情報 AC2を受理する（ステップ S228）。復号処理部 1514は、ライセンスキー Kc を復号処理部 1516に伝達し、再生回路制御情報 AC2をデータバス BS2に出力する。

10 コントローラ 1106は、データバス BS2を介して、再生回路制御情報 AC2を受理して再生の可否の確認を行なう（ステップ S230）。

ステップ S230においては、再生回路制御情報 AC2によって再生不可と判断される場合には、再生セッションは終了される（ステップ S240）。一方、再生可能である場合には、メモリカード 110よりメモリに記録されたリクエスト曲の暗号化されたコンテンツデータ {Data} Kc がデータバス BS3に出力され、メモリインターフェース 1200を介して携帯電話機 100に伝達される（ステップ S232）。

20 携帯電話機 100においては、メモリカード 210から出力されデータバス BS2に伝達された暗号化コンテンツデータ {Data} Kc を復号処理部 1516においてライセンスキー Kc によって復号し、平文化されたコンテンツデータ Data を得ることができる（ステップ S234）。復号された平文化コンテンツデータ Data は音楽再生部 1518によって音楽信号に変換され（ステップ S236）、混合部 1525および端子 1530を介して外部に再生された音楽を出力することによって処理が終了する（ステップ S240）。

25 このような構成とすることで、メモリカード 110側において、コンテンツ再生回路である携帯電話機 100の認証を行なった上で、再生処理を禁止することが可能となる。また、メモリカード内で更新、保持されるアクセス制限情報を反映した再生動作を実行することができる。

再生セッションにおいても、携帯電話機 100およびメモリカード 110でそ

5 れぞれ生成される暗号鍵をやりとりし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信する。この結果、配信セッションと同様に、再生セッションにおいてもデータのそれぞれの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティーを向上させることができる。

次に、図12、図13および図14のフローチャートを用いて、2つのメモリカード間におけるコンテンツデータの複製セッション時の動作（以下、複製動作とも称する）を説明する。

10 図12、図13および図14においては、2つのメモリカード110および112の間で携帯電話機100および102を介した、コンテンツデータおよびキーデータ等の複製動作が説明される。

15 図12、図13および図14においては、携帯電話機100およびメモリカード110についての種類を識別するための自然数を $m = 1$ および $n = 1$ とし、携帯電話機102およびメモリカード112についての種類を識別するため自然数を $m = 2$ および $n = 2$ とする。また、メモリカード110および112を識別するための自然数 i は、それぞれ $i = 1$ および $i = 2$ であるものとする。

20 携帯電話機100およびメモリカード110が送信側であり、携帯電話機102およびメモリカード112が受信側であるものとする。また、携帯電話機102も、メモリカード110と同様の構成を有するメモリカード112が装着されているものとする。以下、メモリカード112の各構成部分については、メモリカード110の対応する部分と同一の符号を用いて説明する。

25 図12を参照して、まず、送信側である携帯電話ユーザ1の携帯電話機100から、携帯電話ユーザ1によりタッチキーパー1108のキー操作等によって、コンテンツ複製リクエストがなされる。（ステップS300）。

生成された複製リクエストは、受信側である携帯電話ユーザ2の携帯電話機102を介してメモリカード112に伝達される。メモリカード112においては、認証データ保持部1500より、メモリカード112に対応する公開暗号鍵KP_{mc}(2)およびクラス証明書C_{mc}(2)が暗号化された認証データ{KP_{mc}(2)//C_{mc}(2)}KP_{ma}が出力される（ステップS302）。

メモリカード112の認証データ {KPmc(2)//Cmc(2)} KPma は、携帯電話ユーザ2の携帯電話機102から送信され、携帯電話ユーザ1の携帯電話機100を経由してメモリカード110に受信される（ステップS304）。

5 メモリカード110においては、復号処理部1408によって、メモリカード112の認証データが復号され、メモリカード112に関するクラス証明書Cmc(2)および公開暗号鍵KPmc(2)が受理される（ステップS306）。コントローラ1420は、データバスBS3を介して復号処理部1408の復号結果に基づいて、認証作業を実行する（ステップS308）。

10 コントローラ1420は、メモリカード112に関する認証データ{KPmc(2)//Cmc(2)} KPma を認証鍵KPmaにて復号した復号結果から、認証データ{KPmc(2)//Cmc(2)} KPma が正規のキーから出力された認証データであることを確認することができる。この確認を実行し、正規のキーから出力された有効な認証データである場合には、公開暗号鍵KPmc(2)およびクラス証明書Cmc(2)を承認して、次のステップS310を実行する。一方、正規のキーから出力されたことが確認できない無効な認証データである場合においては、複製セッションを終了する（ステップS370）。

15 この場合においては、コントローラ1420は、セッションキー発生部1418に対して、複製セッション時に送信側で発生されるセッションキーKs3の出力を指示する。セッションキーへ発生部1418によって生成されたセッションキーKs3は、暗号化処理部1410に伝達される。

20 暗号化処理部1410は、さらに、ステップS306において復号処理部1408によって復号されたメモリカード112の公開暗号鍵KPmc(2)を受けて、KPmc(2)によってセッションキーKs3を暗号化する。これにより、暗号化されたセッションキー{Ks3}Kmc(2)がデータバスBS3に出力される（ステップS312）。データバスBS3に出力された{Ks3}Kmc(2)は、携帯電話機100および携帯電話機102を介してメモリカード112に伝達される。

25 メモリカード112は、メモリカード110から出力された{Ks3}Kmc(2)を受けて、復号処理部1404によってメモリカード112に対応する秘密復号鍵Kmc(2)による復号処理を実行し、送信側のメモリカード110によ

って生成されたセッションキーKs 3 を受理する（ステップS 3 1 4）。

メモリカード1 1 2 のコントローラ1 4 2 0 は、セッションキーKs 3 の受理に応じて、セッションキー発生部1 4 1 8 に対して、複製セッションにおいて受信側で発生されるべきセッションキーKs 2 の生成を指示する。生成されたセッションキーKs 2 は、切換スイッチ1 4 4 6 中の接点 Pf および切換スイッチ1 4 4 4 中の接点 Pc を経由して暗号化処理部1 4 0 6 に伝達される。
5

暗号化処理部1 4 0 6 は、復号処理部1 4 0 4 からステップS 3 1 6 で得られたセッションキーKs 3 を受けて、切換スイッチ1 4 4 4 の接点 Pc と切換スイッチ1 4 4 6 の接点の切換によって得られるセッションキーKs 2 と公開暗号鍵 KPm
10 (2) をセッションキーKs 1 によって暗号化し、{Ks 2 // KPm (2)} Ks 3 をデータバス BS 3 に出力する（ステップS 3 1 6）。データバス BS 3 に出力された暗号化データ {Ks 2 // KPm (2)} は、携帯電話機1 0 2 および1 0 0 を介してメモリカード1 1 0 のデータバス BS 3 に伝達される。

メモリカード1 1 0 においては、データバス BS 3 に伝達された暗号化データを復号処理部1 4 1 2 によってセッションキーKs 3 を用いて復号し、メモリカード1 1 2 に関するセッションキーKs 2 および公開暗号鍵 KPm (2) を受理する（ステップS 3 1 8）。

次に、図1 3 を参照して、メモリカード1 1 0 のコントローラ1 4 2 0 は、セッションキーKs 2 および公開暗号鍵 KPm (2) の受理に応じて、ライセンス情報保持部1 4 4 0 内のアクセス制限情報 AC 1 の確認を実行する。
20

まず、ライセンス情報保持部1 4 4 0 内に格納された対応する再生回数制限情報 Sub_Play を確認し、この値が0であるときは、すでに対応するライセンスは、再生不能の状態であるので複製セッションを終了する（ステップS 3 7 0）。一方、再生回数制限情報 Sub_Play の値が0でない場合には、複製セッションの処理が進められる（ステップS 3 2 0）。

次に、コントローラ1 4 2 0 は、ライセンス情報保持部1 4 4 0 内に格納された対応する所有ライセンス数 Sub_Move を確認し、この値が0もしくはFF(h)であるときは、すでにライセンスが無い状態もしくは、ライセンスが当初から複製禁止の状態であるので複製セッションを終了する（ステップS 3 7 0）。一方、
25

所有ライセンス数 Sub_Move の値が 0 および FF(h) 0 以外であるときには、処理を次のステップに進める（ステップ S 322）。

次のステップにおいては、コントローラ 1420 は、所有ライセンス数 Sub_Move の更新を実行する。ステップ S 324において、複製ライセンス数の入力指示が実行され、残りライセンス数の全てについて複製を指示した場合（ステップ S 326）には、コントローラ 1420 は、ライセンス情報保持部 1440 からアクセス制限情報 AC1 を取得して、所有ライセンス数 Sub_Move の値を 0 に更新する（ステップ S 328）。

また、ステップ S 324において指示された複製ライセンス数が残りライセンス数よりも小さい場合には（ステップ S 326）、コントローラ 1420 は、ライセンス情報保持部 1440 からアクセス制限情報 AC1 を取得して、所有ライセンス数 Sub_Move の値から、入力された複製ライセンス数を減算し、ライセンス情報保持部 1440 内のアクセス制限情報 AC1 を更新する（ステップ S 330）。所有ライセンス数 Sub_Move = 0 となると、以降の再生および複製が禁止される。

コントローラ 1420 は、所有ライセンス数 Sub_Move を更新した後、ライセンス情報保持部 1440 より対応するコンテンツ ID およびライセンス ID を取得する（ステップ S 332）。

さらに、コントローラ 1420 は、複製するコンテンツデータに対応したセッションキー Kc および再生情報に関する暗号化データ { {Kc//AC2} Kcom // ライセンス ID // コンテンツ ID // AC1 } Km (1) の出力をメモリ 1415 に対して指示する。メモリ 1415 から出力された暗号化データ { {Kc//AC2} Kcom // ライセンス ID // コンテンツ ID // AC1 } Km (1) は、復号処理部 1422 によって復号化され、{Kc//AC2} Kcom がデータバス BS4 上に得られる（ステップ S 334）。

ステップ S 332 でライセンス情報保持部 1440 から取得されたライセンス ID、コンテンツ ID およびアクセス制限情報 AC1 と、ステップ S 334 で得られた {Kc//AC2} Kcom は、データバス BS4 から暗号化処理部 1424 に取込まれて暗号化される。暗号化処理部 1424 は、ステップ S 320 において復号処理

部 1 4 1 2 で得られたメモリカード 1 1 2 固有の公開暗号鍵 KPm (2) によって、これらのデータを暗号化し、 $\{ \{ Kc // AC 2 \} Kc \text{ om} // \text{ライセンス ID} // \text{コンテンツ ID} // AC 1 \} Km (2)$ を出力する (ステップ S 3 3 6)。

データバス BS 4 に出力された暗号化データ $\{ \{ Kc // AC 2 \} Kc \text{ om} // \text{ライセンス ID} // \text{コンテンツ ID} // AC 1 \} Km (2)$ は、切換スイッチ 1 4 4 4 中の接点 Pd を介して暗号化処理部 1 4 0 6 に伝達される。暗号化処理部 1 4 0 6 は、復号処理部 1 4 1 2 によって得られたメモリカード 1 1 2 の生成したセッションキー Ks 2 を切換スイッチ 1 4 4 2 の接点 Pb を介して受けて、接点 Pd より受けたデータをセッションキー Ks 2 によって暗号化する。

暗号化処理部 1 4 0 6 は、 $\{ \{ \{ Kc // AC 2 \} Kc \text{ om} // \text{ライセンス ID} // \text{コンテンツ ID} // AC 1 \} Km (2) \} Ks 2$ をデータバス BS 3 に出力する (ステップ S 3 3 8)。ステップ S 3 3 8 においてデータバス BS 3 に出力された暗号化データは、携帯電話機 1 0 0 および 1 0 2 を介して、複製セッションの受信側であるメモリカード 1 1 2 に伝達される。

次に、図 1 4 を参照して、メモリカード 1 1 2 においては、復号処理部 1 4 1 2 においてセッションキー発生部 1 4 1 8 によって生成されたセッションキー Ks 2 による復号が実行され、 $\{ \{ \{ Kc // AC 2 \} Kc \text{ om} // \text{ライセンス ID} // \text{コンテンツ ID} // AC 1 \} Km (2)$ が受理される (ステップ S 3 4 0)。

公開暗号鍵 KPm (2) で暗号化された $\{ \{ Kc // AC 2 \} Kc \text{ om} // \text{ライセンス ID} // \text{コンテンツ ID} // AC 1 \} Km (2)$ は、メモリ 1 4 1 5 に記録される (ステップ S 3 4 2)。さらに、復号処理部 1 4 2 2 において、メモリカード 1 1 2 に固有の秘密復号鍵 Km (2) による復号処理を実行することにより、ライセンス ID、コンテンツ ID およびアクセス制限情報 AC 1 が受理される (ステップ S 3 4 4)。

復号処理部 1 4 2 2 によって得られたライセンス ID、およびコンテンツ ID およびアクセス制限情報 AC 1 は、データバス BS 4 を介してライセンス情報保持部 1 4 4 0 に記録される (ステップ S 3 4 6)。

このようにして、ステップ S 3 3 8 までの処理が正常に終了することによって、再生情報が複製されたことに応答して、携帯電話機 1 0 2 を介してコンテンツデータの複製要求がさらに行なわれる (ステップ S 3 4 8)。

コンテンツデータの複製要求は携帯電話機 100 を経由してメモリカード 110 に伝達され、これに応答して、メモリカード 110 中のメモリ 1415 より対応する暗号化コンテンツデータの {Data} Kc と付加情報 Data-inf とがデータバス BS3 に出力される（ステップ S 350）。

5 データバス BS3 に出力されたこれらのデータは、携帯電話機 100 および携帯電話機 102 を介してメモリカード 112 に入力され、メモリカード 112 中のメモリ 1415 に記録される（ステップ S 352）。

10 暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf の記録が終了すると、携帯電話機 102 を介して複製受理が送信される（ステップ S 354）。これにより、メモリカード 112 および対応する携帯電話機 102 において正常に再生セッションが実行されれば、携帯電話機 102 によって、メモリカード 112 に記録された暗号化コンテンツデータを再生して音楽を聴取することが可能となる。

15 送信側の携帯電話機 100 においては、携帯電話機 102 から送信された複製受理を受信して（ステップ S 356）する。

複製受理を受信すると、メモリカード 110 においては、ライセンス情報保持部 1440 内の所有ライセンス数 Sub_Move を確認し（ステップ S 358）、この値が 0 である場合、すなわちライセンスが無くなった場合においては、暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf の消去もしくは保持のいずれかをタッチキー部 1108 から入力することを要求する（ステップ S 360）。

したがって、ライセンスの無くなったコンテンツデータを消去したい場合には、タッチキー部 1108 より消去を指示することにより（ステップ S 362）、メモリカード 110 内のメモリ 1415 において、対応する暗号化コンテンツデータ {Data} Kc、付加情報 Data-inf を消去することができる（ステップ S 364）。なお、ライセンス情報保持部 1440 内に記録された対応するコンテンツ ID 等の再生情報は、ステップ S 328 にてアクセス制限情報 AC1 内の Sub_Move が更新され、Sub_Move=0 となっているため、以降の再生セッションおよび複製セッションは禁止されている。

一方、コンテンツデータ等の保持が指示された場合および、ライセンス情報保持部中の所有ライセンス数 Sub_Move が 0 以外である場合（すなわち、ライセンスが残っている場合）においては、ステップ S 3 6 4 はスキップされ、複製処理はこの段階で終了する（ステップ S 3 6 6）。

- 5 正常に複製セッションが行なわれた場合の複製処理終了ステップ S 3 6 6、もしくは認証チェック等によって複製セッションが中止された場合にはステップ S 3 0 8、S 3 2 0 および S 3 2 2 からスキップされて複製セッション全体の処理が終了する（S 3 7 0）。

このような構成とすることにより、複製セッションにおいても、受信回路側のコンテンツ再生回路（携帯電話機）およびメモリカードの認証を事前にチェックした後に、ライセンスキーや暗号化コンテンツデータの複製を実行する構成とするので、認証されていない再生回路（携帯電話機）もしくはメモリカードに対するコンテンツデータの複製の禁止を行なうことができる。

また、複製動作におけるライセンスの変化をメモリカード内で保持されるアクセス制限情報 AC 1 (Sub_Move) にメモリカードが独自に反映させる構造になっている。したがって、再生情報および暗号化コンテンツデータを無制限に複製することを防止できる。

なお、暗号化コンテンツデータ {Data} Kc をメモリ 1 4 1 5 に記録された状態から、新たに配信サーバ 3 0 をアクセスし、再生情報のみの配信のみを受けることが可能な配信サービスが考えられる。このように、再生情報のみの配信を受ければ、再び、暗号化コンテンツデータ {Data} Kc を再生して、音楽を聴取できるようになる。

再生情報のみの配信処理は、フローチャートには図示されていないが、配信セッションにおける図 9 および図 10 において、暗号化コンテンツデータの授受に関する、ステップ S 1 4 6、S 1 4 8、S 1 5 0 および S 1 5 2 を実行しない処理に相当するため、ここでは詳細な説明を繰り返さない。

また、ステップ S 3 2 8 において、複製を目的としてライセンス情報保持部 1 4 4 0 内の再生情報を取得すると、アクセス制限情報 AC 1 内の Sub_Move の値を 0 に更新すると説明したが、当該データをライセンス情報保持部 1 4 4 0 から消

去しても同様の効果が得られる。

以上説明したように、実施の形態 1 に従う情報配信システムによれば、所有ライセンス数および再生可能回数といったアクセス制限情報を、配信サーバを介さずにメモリカード内の TRM 領域で保持更新することができる。この結果、ファイ 5 イルシステムやアプリケーションプログラム等によって上位レベルからアクセス制限情報を改ざんすることができない構成とすることができるので、コンテンツデータに対する著作権保護をより強固なものとすることができます。

(実施の形態 2)

実施の形態 2 のデータ配信システムにおいては、実施の形態 1 のデータ配信シ 10 ステムの構成と異なって、再生回路共通の秘密鍵 K_{com} によって復号可能な暗号化を行なわない点を特徴とする。

すなわち、実施の形態 2 のデータ配信システムは、実施の形態 1 のデータ配信システムが具備する配信サーバ 30 内のライセンスサーバ 10 に代えてライセンスサーバ 11 を備える点で異なる。また、実施の形態 2 のデータ配信システムに 15 おける携帯電話機の構成は、図 5 で説明した携帯電話機 100 の構成に代えて携帯電話機 101 の構成が採用される。

図 15 を参照して、ライセンスサーバ 11 は、ライセンスサーバ 10 と比較して、再生回路共通の秘密鍵 K_{com} 保持部 322 と、秘密鍵 K_{com} による暗号化処理部 324 を具備しない点で異なる。すなわち、ライセンスサーバ 11 においては、配信制御部 315 が出力するライセンスキー K_c および再生回路制御情報 AC2 は、直接暗号化処理部 326 に伝達される。その他の回路構成および動作については図 4 に示すライセンスサーバ 10 と同様であるので説明は繰返さない。

以降、ライセンスサーバ 11、認証サーバ 12 および配信キャリア 20 を合わせて配信サーバ 31 と総称することとする。

図 16 を参照して、実施の形態 2 に従うデータ配信システムにおいて使用される携帯電話機携帯電話機 101 は、実施の形態 1 で説明した携帯電話機 100 の構成と比較して、再生回路共通の秘密鍵 K_{com} を保持する K_{com} 保持部 1512 と秘密鍵 K_{com} による復号処理部 1514 を具備しない点で異なる。

すなわち、携帯電話機 101 においては、配信サーバ 31 において秘密鍵

K_{com} による暗号化処理が施されていないことに対応して、セッションキーK_{s 4}による復号処理を実行する復号処理部 1510 によって直接ライセンスキーK_cが得られるため、これを復号処理部 1510 に直接与える構成となる。その他の回路構成および動作については携帯電話機 100 の場合と同様であるので説明は繰返さない。

また、実施の形態 2 に従うデータ配信システムにおいて使用されるメモリカードについては、図 6 に示すメモリカード 110 と同一の構成であるので説明は繰返さない。

次に、再生回路共通の秘密鍵 K_{com} による暗号化を省略することによる、配信、
10 再生および複製の各セッションにおける動作の差異についてフローチャートで説明する。

次に、図 17 のフローチャートを用いて、実施の形態 2 に従うデータ配信システムにおける配信動作を説明する。図 17 においては、図 9 および図 10 で示した実施の形態 1 に従うデータ配信システムにおける配信動作のフローチャートと異なる点について説明する。

図 17 においては、携帯電話ユーザが、メモリカード 110 を用いることで、実施の形態 2 に従う配信サーバ 31 から、携帯電話機 101 を介して音楽データであるコンテンツデータの配信を受ける場合の動作が説明される。

図 17 を参照して、実施の形態 2 に従う配信動作においても、ステップ S 10
20 0 から S 128 までの処理は、図 10 で説明したフローチャートと同様であるので、図示および詳細な説明は繰り返さない。

図 15 で説明したように、ステップ S 128 で得られるライセンスキー K_c および再生回路制御情報 AC 2 は、秘密鍵 K_{com} による暗号化を施されることなくメモリカード 110 固有の公開暗号鍵 K_{Pm} (1) によって暗号化されるので、ステップ S 130 は省略される。

以下、ステップ S 128 に続いて、ステップ S 132～S 142 に代えて、ステップ S 132a～S 142a が実行される。ステップ S 132a～S 142a のそれぞれにおいては、ステップ S 132～S 142 において取り扱われるライセンスキー K_c および再生回路制御情報 AC 2 が、暗号化された形 {K_c//AC 2}

Kcom から、そのままの形である Kc および AC 2 に代えられて取扱われる点が異なる。その他の暗号化および復号処理については既に図 10 で説明したのと同様であるので説明は繰返さない。

5 図 18 には、実施の形態 2 に従うデータ配信システムにおける再生動作のフローが示される。

図 18 を参照して、実施の形態 2 に従うデータ配信システムにおいて使用される携帯電話機携帯電話機 101 による再生動作においては、図 11 に示した実施の形態 1 に従う再生動作と比較して、ステップ S 222～S 226 に代えて、ステップ S 222a～S 226a が実行される点で異なる。

10 ステップ S 222a～S 226a のそれぞれにおいては、ステップ S 222～S 226 において取り扱われるライセンスキー Kc および再生回路制御情報 AC 2 が、暗号化した形 {Kc//AC 2} Kcom から、そのままの形である Kc//AC 2 に代えられて取扱われる点が異なる。その他の暗号化および復号処理については既に図 11 で説明したのと同様であるので説明は繰返さない。また、他のステップ 15 については図 11 と同様であるので説明は繰返さない。

図 19 および図 20 には、実施の形態 2 に従うデータ配信システムにおける複製動作のフローが示される。

20 図 19 および図 20 においては、2つのメモリカード 110 および 112 の間で、実施の形態 2 に従う携帯電話機 101 および 103 を介してコンテンツデータおよびキーデータ等の複製を行なう処理を説明する。

携帯電話機 101 およびメモリカード 110 についての種類を識別するための自然数を $m = 1$ および $n = 1$ とし、携帯電話機 103 およびメモリカード 112 についての種類を識別するため自然数を $m = 2$ および $n = 2$ とする。また、メモリカード 110 および 112 を識別するための自然数 i は、実施の形態 1 と同様 25 に、それぞれ $i = 1$ および $i = 2$ であるものとする。

図 19 および 20 においては、図 12 から図 14 に示した実施の形態 1 に従う複製動作のフローチャートと異なる点について説明する。

図 12 で説明したステップ S 300 から S 338 までの処理は、実施の形態 2 に従う複製動作においても同様に実行されるので、図示および詳細な説明は繰り

返さない。

図19および図20を参照して、実施の形態2に従うデータ配信システムにおける複製セッションにおいては、図13および図14に示すステップS334～S344に代えて、ステップS334a～S344aが実行される点、およびステップS228が省略される点で異なる。
5

ステップS334a～S344aのそれぞれにおいては、ステップS334～S344において取り扱われるライセンスキーKc および再生回路制御情報 AC2 が、暗号化された形 {Kc//AC2} Kcom から、そのままの形である Kc および AC2 に代えられて取扱われる点が異なる。また、秘密鍵 Kcom によって暗号化されることなく、ライセンスキーKc および再生制限情報 AC2 が与えられるので、ステップS228は省略される。
10

その他の暗号化および復号処理については既に図13および図14で説明したのと同様であるので説明は繰返さない。

15 その他のステップについては図13および図14と同様であるので説明は繰返さない。

このような構成とすることによって、再生回路に共通な秘密鍵 Kcom を用いない構成としても、実施の形態1に従うデータ配信システムと同様の効果を享受するデータ配信システムを構築することが可能である。

[実施の形態3]

20 実施の形態3に従うデータ配信システムにおいては、実施の形態2のデータ配信システムの構成とは異なって、ライセンスキーKc および再生回路制御情報 AC2 がメモリカードにおいて、暗号化されることなく平文にて記録される点を特徴とする。

25 すなわち、実施の形態3に従う配信システムは、実施の形態2のメモリカード110に代えて、メモリカード210を備える点で異なる。配信サーバ31および携帯電話機101の構成は同一であるため説明は繰返さない。

図21を参照して、メモリカード210は、メモリカード110と比較して、データバスBS4を介してメモリ1415とデータの授受が行なわれない点、および、ライセンスキーKc と再生回路制御情報 AC2 を格納する再生情報制御部14

30を備える点で異なる。再生情報保持部1430は、必ずTRM領域内に設けられ、データバスBS4との間でデータの授受が可能である。

実施の形態2の場合とは異なり、公開暗号鍵KPm(1)にて暗号化された状態でメモリカードに伝達される、ライセンスキーKcおよび再生回路制御情報AC2は、
5 メモリ1415に直接格納されない。すなわち、ライセンスキーKcおよび再生制御情報AC2は、復号処理部1422によって復号された後、データバスBS4を介して、平文にて再生情報保持部1430に保持される。

図22を参照して、再生情報保持部1430は、ライセンス情報保持部1440と対応したN個のバンクを有し、各ライセンスに対応するライセンスキーKc
10 および再生回路制御情報AC2をバンクごとに保持する。このとき、ライセンス情報保持部1440に保持された、同一のライセンスに対するライセンスID、コンテンツIDおよびアクセス制限情報AC1を保持したバンクと対応したバンクを用いる。

15 その他の部分の構成については、メモリカード110と同様であるため詳細な説明は省略する。なお、メモリカードに対応して定められる自然数i、およびmは、本来、メモリカード110と同一の値になり得ないが、説明を簡略化するために、以下においては、これらの自然数iおよびmは、実施の形態1および2におけるメモリカード110と同様に、i=1およびm=1であるものとして説明する。

20 実施の形態3に従う配信動作については、フローチャートは図示されていないが、実施の形態2における図17の配信動作時のフローチャートにおいて、ライセンスの記録を行なうステップS140aおよびS142aにおける処理を変更すればよい。

25 ステップS140aに相当するステップにおいては、暗号化データ{Kc//AC1//ライセンスID//コンテンツID//AC2}Km(1)を復号処理部1422において秘密復号鍵Km(1)を用いて復号し、得られたライセンスキーKcおよび再生回路制御情報AC2を再生情報保持部1430に記録する。さらに、ステップS142aに相当するステップにおいては、ステップS140aに相当するステップにおける復号処理で得られたライセンスID、コンテンツIDおよびアクセス制限

情報 AC1 を、ライセンス保持部情報保持部 1440 中の再生情報保持部 1430 と対応するバンクに記録する。再生動作の他のステップにおける処理は、実施の形態 2 の場合と同様であるため説明は繰り返さない。

同様に、実施の形態 3 に従う再生動作については、フローチャートは図示されていないが、実施の形態 2 における図 18 の再生動作時のフローチャートにおいて、メモリ 1415 からライセンスキーキー Kc、再生回路制御情報 AC2 を取得するステップ S222a における処理内容が変更される。すなわち、ステップ S222a に相当するステップにおいて、再生情報保持部 1430 からライセンスキーキー Kc、再生回路制御情報 AC2 を取得する。再生動作の他のステップにおける処理は、実施の形態 2 の場合と同様であるため説明は繰り返さない。

このように、実施の形態 3 に従う配信システムは、実施の形態 2 に従う配信システムに対してメモリカード 210 の内部処理が異なるのみであり、実施の形態 2 と互換性があり、相互に運用することができる。

同様に、実施の形態 3 に従う複製動作については、フローチャートが図示されていないが、配信動作および再生動作と同様に、実施の形態 2 における図 19 および図 20 の複製動作時のフローチャートにおいて、メモリ 1415 からライセンスキーキー Kc、再生回路制御情報 AC2 を取得するステップ S334a、ライセンスの記録を行なうステップ S342a および S344a における処理を変更すればよい。すなわち、ステップ S342a に相当するステップにおいては、暗号化データ {Kc//AC2//ライセンス ID//コンテンツ ID//AC1} Km(2) を復号処理部 1422 において秘密復号鍵 Km(2) を用いて復号し、得られたライセンスキーキー Kc および再生回路制御情報 AC2 を再生情報保持部 1430 に記録する。さらに、ステップ S344a に相当するステップにおいては、ステップ S342a に相当するステップにおける復号処理で得られたライセンス ID、コンテンツ ID およびアクセス制限情報 AC1 を、ライセンス保持部情報保持部 1440 中の再生情報保持部 1430 と対応するバンクに記録する。

なお、実施の形態 2 における配信システムにおいては、メモリカード内の動作が異なるのみであるため、実施の形態 2 のメモリカード 110 と実施の形態 3 のメモリカード 210 とは相互互換のあるメモリカードであり、その意味において

実施の形態 2 と実施の形態 3 との配信システムは同一の配信システムで運用することができる。

また、このような実施の形態 3 に従うメモリカード 210 の適用は、実施の形態 1 に従う配信システムとの組合せにおいても実行することができる。すなわち、
5 ライセンスキー Kc および再生回路制御情報 AC2 を鍵 Kcom によって暗号化された
{Kc//AC2} Kcom の状態で、再生情報保持部 1430 に記録することも可能である。

以下に、このような場合における実施の形態 1 に従う配信システムにおける処理動作からの変更点を説明する。

10 実施の形態 3 を実施の形態 1 と組合せた場合の配信動作については、実施の形態 1 における図 10 フローチャートにおいて、ライセンスの記録を行なうステップ S140 および S142 における処理を変更すればよい。

15 ステップ S140 に相当するステップにおいては、暗号化データ ({Kc//AC2} Kcom//ライセンス ID//コンテンツ ID//AC1} Km(1) を復号処理部 1422 において秘密復号鍵 Km(1) を用いて復号し、得られたライセンスキー Kc および再生回路制御情報 AC2 を再生情報保持部 1430 に記録する。さらに、ステップ S1
42 に相当するステップにおいては、ステップ S140 に相当するステップにおける復号処理で得られたライセンス ID、コンテンツ ID およびアクセス制限情報 AC1 を、ライセンス保持部情報保持部 1440 中の再生情報保持部 1430 と対
20 応するバンクに記録する。再生動作の他のステップにおける処理は、実施の形態 1 の場合と同様であるため説明は繰り返さない。

25 同様に、実施の形態 3 を実施の形態 1 と組合せた場合の再生動作については、実施の形態 1 における図 11 の再生動作時のフローチャートにおいて、メモリ 1415 からライセンスキー Kc、再生回路制御情報 AC2 を取得するステップ S222 における処理内容が変更される。すなわち、ステップ S222 に相当するステップにおいて、ライセンスキー Kc、再生回路制御情報 AC2 を {Kc//AC2} Kcom の形で再生情報保持部 1430 から取得する。再生動作の他のステップにおける処理は、実施の形態 1 の場合と同様であるため説明は繰り返さない。

同様に、実施の形態 3 を実施の形態 1 と組合せた場合の複製動作については、

配信動作および再生動作と同様に、実施の形態 1 における図 1 3 および図 1 4 の複製動作時のフローチャートにおいて、メモリ 1 4 1 5 からライセンスキー Kc および再生回路制御情報 AC2 を {Kc//AC2} Kcom の形で取得するステップ S 3 3 4 、ライセンスの記録を行なうステップ S 3 4 2 および S 3 4 4 における処理を変更すればよい。すなわち、ステップ S 3 4 2 に相当するステップにおいては、暗号化データ ({Kc//AC2} Kcom // ライセンス ID // コンテンツ ID // AC1) Km(2) を復号処理部 1 4 2 2 において秘密復号鍵 Km(2) を用いて復号し、得られた {Kc//AC2} Kcom を再生情報保持部 1 4 3 0 に記録する。さらに、ステップ S 3 4 4 に相当するステップにおいては、ステップ S 3 4 2 に相当するステップにおける復号処理で得られたライセンス ID 、コンテンツ ID およびアクセス制限情報 AC1 を、ライセンス保持部情報保持部 1 4 4 0 中の再生情報保持部 1 4 3 0 と対応するバンクに記録する。

このように、実施の形態 3 に従う配信システムは、実施の形態 1 に従う配信システムに対してメモリカード 2 1 0 の内部処理が異なるのみであり、実施の形態 1 と互換性があり、相互に運用することができる。

なお、実施の形態 1 における配信システムにおいては、メモリカード内の動作が異なるのみであるため、実施の形態 1 のメモリカード 1 1 0 と実施の形態 3 のメモリカード 2 1 0 とは相互互換のあるメモリカードであり、その意味において実施の形態 1 と実施の形態 3 とを組合せて同一の配信システムで運用することができる。

なお、図 2 1 においては、TRM 領域に配置される再生情報保持部 1 4 3 0 およびライセンス保持部情報保持部 1 4 4 0 を独立した機能を有するブロックとして示したが、両者を共通のメモリとして配置することも可能である。また、実施の形態 1 で述べたように、メモリ 1 4 1 5 を TRM 領域に配置することも可能であるが、この場合において、メモリ 1 4 1 5 、再生情報保持部 1 4 3 0 およびライセンス保持部情報保持部 1 4 4 0 を共通の同一メモリ上に設けることも可能である。

なお、以上で説明したすべての実施の形態においては、複製動作時において、一度に複数のライセンスが複製できる構成について説明したが、一度の複製動作では、1 つのライセンスが複製可能なように構成することも可能である。この場

合においては、実施の形態1における図13ならびに、実施の形態2および3における図20に示したフローチャートからステップS324を省略して、ステップS326において、複製ライセンス数が“1”であるとして判断する処理とすればよい。

5 また、ライセンスの複製は、アクセス制限情報AC1の所有ライセンス数Sub_moveの制約上必ず制限を受けるように説明したが、コンテンツデータの著作権を所有する著作権者が自由に複製することを許可した場合には、自由な複製が可能となる。この場合には、たとえば所有ライセンス数Sub_moveに新たな値、たとえばFE(h)を追加して、Subh_move=FE(h)であれば複製自由とし、図13に示したフローチャート中のステップS322の判断処理において、Sub_move=FE(h)の場合に新しい分岐を設けて、ライセンス処理部からAC1を取得する処理を得た後、Sub_move=FE(h)であればステップS332に移行する処理を行なうことによって実現することができる。
10

また、以上で説明したすべての実施の形態においては、配信動作において、携帯電話機100から2つの認証データ{KPmc(1)//Cmc(1)}KPmaおよび{KPP(1)//CP(1)}KPmaを送信して配信サーバ10において2つの認証データに対して認証処理をする構成について説明した。

しかし、メモリカード110は着脱可能であることから、音楽を再生する場合にコンテンツ再生回路が必ずしも配信を受けた携帯電話機100である必然性がない。さらに、メモリカード100が再生動作において再生するコンテンツ再生回路の認証データ{KPP(1)//CP(1)}KPmaによって認証処理を行なっているので、配信サーバ10においてコンテンツ再生回路の認証データ{KPP(1)//CP(1)}KPmaによってコンテンツ再生回路(携帯電話機100)の認証処理を行なわなくともセキュリティの低下にはつながらない。

25 したがって、配信サーバ10に対して、メモリカード100の認証データ{KPmc(1)//Cmc(1)}KPmaのみを送信し、配信サーバ10においては、配信先のメモリカード110の認証データ{KPmc(1)//Cmc(1)}KPmaのみを中心にして復号し認証処理を行なう構成としても同様の効果を得ることができる。

この場合には、すべての実施の形態が参照する図9に示されたフローチャート

において、ステップS104、S106、S108、S110の各処理において、携帯電話機（コンテンツ再生回路）100の認証データ{KPp(1)//Cp(1)}KPma、公開暗号鍵KPp(1)およびクラス証明書Cp(1)に対する処理を省略することによって、コンテンツ再生回路に対する認証を省略した認証処理を行なうことができる。

5 今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

10 産業上の利用可能性

この発明によるデータ配信システムおよび記録装置は、携帯電話機のような移動通信端末を利用したデータ配信に用いることができる。

請求の範囲

1. データ配信システムであって、
暗号化コンテンツデータ ($\{Data\} Kc$) と、前記暗号化コンテンツデータを復号して平文のコンテンツデータ (Data) を得るための復号鍵であるライセンスキー (Kc) を配信するためのコンテンツ供給装置 (10, 11) と、
前記コンテンツ供給装置からの前記配信を受ける複数の端末 (100, 101) とを備え、
前記コンテンツ供給装置は、
外部との間でデータを授受するための第1のインターフェース部 (350) と、
前記配信が要求された場合において、アクセス制限情報 (AC1) を生成して、
少なくとも前記ライセンスキーを含む再生情報 ($Kc//AC2$, $\{Kc//AC2\} Kcom$) と前記アクセス制限情報とを前記第1のインターフェース部を介して出力するための配信制御部 (315) とを含み、
各前記端末は、
外部との間でデータを授受するための第2のインターフェース部 (1102) と、
前記第2のインターフェース部を介して、前記暗号化コンテンツデータと前記再生情報と前記アクセス制限情報を受けて記録する配信データ解読部 (110, 210) とを含み、
前記配信データ解読部は、
前記暗号化コンテンツデータ、前記再生情報および前記アクセス制限情報を記録するための記憶部 (1415, 1430, 1440) と、
外部から前記再生情報の出力が指示された場合に、前記記憶部に記録された前記アクセス制限情報に基づいて前記出力の可否を判断する制御部 (1420) とを有する、データ配信システム。
2. 各前記端末 (100, 101) は、コンテンツ再生部をさらに含み、
前記コンテンツ再生部は、
外部からコンテンツデータの再生動作が指示された場合において、前記配信データ解読部 (110, 210) から前記再生情報 ($Kc//AC2$, $\{Kc//AC2\} Kcom$) および前記暗号化コンテンツデータ ($\{Data\} Kc$) を受けて、前記ライセンスキー

(Kc) によって前記暗号化コンテンツデータを復号して再生するコンテンツデータ再生部（1516, 1518）を有し、

前記アクセス制限情報（AC1）は、前記配信データ解読部から前記コンテンツ再生部への、前記再生情報の出力回数を制限する再生制御情報（Sub_Play）を含み、

前記制御部（1420）は、前記再生動作が指示された場合において、前記記憶部に記録された前記再生制御情報に基づいて、前記再生情報の出力の可否を判断するとともに、前記再生情報の出力後、必要に応じて前記再生制御情報を更新できる、請求の範囲第1項に記載のデータ配信システム。

10 3. 前記アクセス制限情報（AC1）は、前記配信データ解読部（110, 210）から他の配信データ解読部（112）に対しての、前記再生情報（Kc//AC2, {Kc//AC2} Kcom）の複製可能回数を制限する複製制限情報（Sub_Move）を含み、

前記制御部（1420）は、他の配信データ解読部に対して前記再生情報を複製する複製動作が外部から指示された場合において、前記記憶部に記録された前記複製制限情報に基づいて前記再生情報の出力の可否を判断するとともに、前記再生情報の出力後、必要に応じて前記複製制限情報を更新できる、請求の範囲第1項に記載のデータ配信システム。

4. 前記コンテンツ供給装置（10, 11）は、

20 認証鍵（KPma）によって復号可能な状態に暗号化された、前記配信データ解読部（110, 210）に対応して予め定められる第1の公開暗号鍵（KPmc(m)）を、前記第1のインターフェース部（350）を介して受けて復号処理するための第1の復号処理部（312）と、

前記暗号化コンテンツデータおよび前記ライセンスキーの少なくとも一方の通信ごとに更新される第1の共通鍵（Ks1）を生成する第1のセッションキー生成部（316）と、

前記第1の共通鍵によって暗号化されて、前記第1のインターフェース部を介して返信される第2の公開暗号鍵（KPm(i)）および第2の共通鍵（Ks2）を復号抽出するためのセッションキー復号部（320）と、

前記再生情報（Kc//AC2, {Kc//AC2} Kcom）および前記アクセス制限情報（AC1）を、

前記セッションキー復号部により復号された前記第2の公開暗号鍵によって暗号化する第1のライセンスデータ暗号化処理部（326）と、

前記第1のライセンスデータ暗号化処理部の出力を、前記セッションキー復号部により復号された前記第2の共通鍵によってさらに暗号化して前記第1のインターフェース部に与え配信するための第2のライセンスデータ暗号化処理部（328）とをさらに含み、

前記配信データ解読部（110，210）は、

前記認証鍵によって復号可能な状態に暗号化された、前記配信データ解読部に対応して定められる前記第1の公開暗号鍵を保持し、少なくとも前記ライセンスキーを受信する場合に出力する第1の認証データ保持部（1400）と、

前記第1の公開暗号鍵によって暗号化されたデータを復号するための第1の秘密復号鍵（Kmc(m)）を保持する第1の鍵保持部（1402）と、

前記第1の公開暗号鍵によって暗号化された前記第1の共通鍵を受けて、前記第1の秘密復号鍵によって復号処理するための第1の復号処理部（1404）と、

前記第2の公開暗号鍵を保持する第2の鍵保持部（1416）と、

前記暗号化コンテンツデータおよび前記ライセンスキーの少なくとも一方の通信ごとに更新される前記第2の共通鍵（Ks2）を生成する第2のセッションキー発生部（1418）と、

前記第2の共通鍵および前記第2の公開暗号鍵を前記第1の共通鍵によって暗号化し、前記第2のインターフェース部（1202）に出力するための第1の暗号化処理部（1406）と、

前記コンテンツ供給装置から配信される、前記第2の共通鍵および前記第2の公開暗号鍵によって暗号化された、前記再生情報および前記アクセス制限情報を受けて、前記第2の共通鍵によって復号するための第2の復号処理部（1412）と、

前記第2の公開暗号鍵によって暗号化されたデータを復号するための第2の秘密復号鍵（Km(i)）を保持する第3の鍵保持部（1421）と、

暗号化された、前記再生情報および前記アクセス制限情報を、第2の秘密復号鍵によって復号するための第3の復号処理部（1422）とをさらに有し、

前記記憶部（1415, 1430, 1440）は、前記再生情報を、前記第2の公開暗号鍵によって暗号化された状態および前記第3の復号処理部によって復号された状態のいずれか一方の状態で記録するための第1の記憶ブロック（1415, 1430）と、

5 前記アクセス制限情報を記録するための第2の記憶ブロック（1440）とを有する、請求の範囲第1項に記載のデータ配信システム。

5. 前記第2のセッションキー発生部（1418）は、外部から指示されるコンテンツデータの再生動作に応じて、第3の共通鍵（Ks3）を生成し、

10 前記記憶部（1415, 1430, 1440）は、前記制御部（1420）に制御されて、前記再生動作が指示されるのに応じて、前記暗号化コンテンツデータ（{Data} Kc）および前記再生情報を出力し、

前記第3の復号処理部（1422）は、前記再生動作において、前記第1の記憶ブロックから出力された前記再生情報が暗号化されている場合に、復号を行なって前記再生情報（Kc//AC2, {Kc//AC2} Kcom）を抽出し、

15 前記第2の復号処理部（1412）は、前記再生動作において、前記第3の共通鍵によって暗号化されて前記端末から返信されるデータを復号して、前記再生動作を行なう前記端末において前記再生情報の通信ごとに更新される第4の共通鍵（Ks4）を抽出し、

20 前記第1の暗号化処理部（1406）は、前記再生動作において、前記第3の復号処理部および前記第1の記憶ブロックのいずれか一方から前記再生情報を受けて、前記第2の復号処理部（1412）で抽出された前記第4の共通鍵によって暗号化し、

各前記端末（100, 101）は、コンテンツ再生部をさらに備え、

前記コンテンツ再生部は、

25 前記認証鍵によって復号可能な状態に暗号化された、前記コンテンツ再生部に対応して予め定められる、第3の公開暗号鍵（KPp(i)）を保持し、前記再生動作に応じて前記配信データ解読部に対して出力する第2の認証データ保持部（1500）と、

前記第4の共通鍵を生成する第3のセッションキー発生部（1508）と、

前記配信データ解読部から送信される、前記第4の共通鍵によって暗号化された前記再生情報から前記再生情報を復号抽出するための第4の復号処理部（1510）と、

5 前記再生動作が指示された場合において、前記配信データ解読部（110, 210）からの前記暗号化コンテンツデータを受けて、前記再生情報に含まれる前記ライセンスキー（Kc）により前記暗号化コンテンツデータを復号して再生するためのコンテンツデータ再生部（1516, 1518）と、

10 前記第3の公開暗号鍵によって暗号化されたデータを復号化するための第3の秘密復号鍵（Kp(i)）を保持する第4の鍵保持部（1502）と、

前記第3の公開暗号鍵によって暗号化されて前記配信データ解読部から返信されるデータを復号して前記第3の共通鍵を得るための第5の復号処理部（1504）と、

15 前記第5の復号処理部から受ける前記第3の共通鍵によって、前記第4の共通鍵を暗号化して前記配信データ解読部に対して出力する第2の暗号化処理部（1506）とを有し、

前記配信データ解読部は、

暗号化された前記第3の公開暗号鍵を前記コンテンツ再生部から受けて、前記認証鍵によって復号処理するための認証処理部（1408）と、

20 前記制御部に制御されて、前記認証処理部から受ける前記第3の公開暗号鍵によって前記第3の共通鍵を暗号化して、対応する前記コンテンツ再生部に対して出力する第3の暗号化処理部（1410）とをさらに有し、

前記アクセス制限情報（AC1）は、前記配信データ解読部から前記コンテンツデータ再生部への、前記再生情報の出力回数を制限する再生制御情報（Sub_Move）を含み、

25 前記制御部（1420）は、前記再生動作が指示された場合において前記配信データ解読部の各部の動作を制御し、前記第2の記憶ブロックに記録された前記再生制御情報に基づいて前記再生情報の出力の可否を判断するとともに、前記再生情報の出力後、必要に応じて前記再生制御情報を更新可能である、請求の範囲第4項に記載のデータ配信システム。

6. 前記認証処理部（1408）は、他の配信データ解読部（102）に対して前記再生情報を複製する複製動作が外部から指示された場合において、前記他の配信データ解読部に対応する前記第1の公開暗号鍵（KP_{mc(m)}）を復号処理によって取得し、
- 5 前記配信データ解読部および前記他の配信データ解読部にそれぞれ対応する複数の前記第2のセッションキー発生部は、外部から指示される前記複製動作に応じて、前記第3および第2の共通鍵（K_{s3}, K_{s2}）をそれぞれ生成し、
前記第3の暗号化処理部（1410）は、前記複製動作において、前記他の配信データ解読部に対応する前記第1の公開暗号鍵によって、前記配信データ解読
10 部に対応する前記第3の共通鍵を暗号化して前記他の配信データ解読部に対して出力し、
前記第2の復号処理部（1412）は、前記複製動作において、前記配信データ解読部に対応する前記第3の共通鍵で暗号化されて前記他の配信データ解読部から返信されるデータを復号して、前記他の配信データ解読部で生成された前記
15 第2の共通鍵および前記他の配信データ解読部に対応する前記第2の公開暗号鍵（KP_{m(i)}）を取得し、
前記第1の記憶ブロック（1415, 1430）は、前記制御部（1420）に制御されて、前記複製動作が指示されるのに応じて、前記再生情報を出力し、
前記第3の復号処理部（1422）は、前記複製動作において、前記第1の記憶ブロックから出力された前記再生情報が暗号化されている場合に、復号を行なって前記再生情報（K_c//AC2, {K_c//AC2} K_{com}）を抽出し、
前記配信データ解読部（110, 210）は、
前記複製動作が外部から指示された場合において、前記第3の復号処理部および前記第1の記憶ブロックのいずれか一方から受けた前記再生情報を、前記他の配信データ解読部に対応する前記第2の公開暗号鍵によって暗号化するための第
25 4の暗号化処理部（1424）をさらに有し、
前記第1の暗号化処理部（1406）は、前記複製動作において、前記第2の復号処理部（1412）によって取得された前記第2の共通鍵と、前記第4の暗号化処理部の出力とを受けて、前記第4の暗号化処理部の出力を前記第2の共通

鍵によってさらに暗号化して前記他の配信データ解読部に出力し、

前記アクセス制限情報(AC1)は、前記配信データ解読部から他の配信データ解読部に対しての、前記再生情報の複製可能回数を制限する複製制限情報(Sub_move)を含み、

5 前記制御部(1420)は、前記複製動作時において前記配信データ解読部の各部の動作を制御し、前記第2の記憶ブロックに記録された前記複製制限情報に基づいて前記再生情報の出力の可否を判断するとともに、前記再生情報の出力後、必要に応じて前記複製制限情報を更新する、請求の範囲第5項に記載のデータ配信システム。

10 7. 前記コンテンツ供給装置(10)は、

前記コンテンツ再生部にて再生可能な共通秘密鍵(Kcom)を保持する第5の鍵保持部(322)と、

15 前記再生情報(Kc//AC2, {Kc//AC2} Kcom)を前記共通秘密鍵によって暗号化し、前記第1のライセンスデータ暗号化処理部(326)に対して出力する第3のライセンスデータ暗号化部(324)とをさらに含み、

前記コンテンツ再生部は、

前記共通秘密鍵を保持する第6の鍵保持部(1512)と、

20 前記第4の復号処理部(1510)の出力を受けて、前記第6の鍵保持部に保持された前記共通秘密鍵によって前記再生情報を復号し、前記ライセンスキーキ(Kc)を抽出して前記コンテンツデータ再生部(1516, 1518)に対して出力するための第6の復号処理部(1514)をさらに有する、請求の範囲第5項に記載のデータ配信システム。

8. 前記コンテンツ供給装置(10)は、

25 前記コンテンツデータ再生部にて再生可能な第4の公開暗号鍵を保持する第5の鍵保持部と、

前記再生情報を前記第4の公開暗号鍵にて暗号化し、前記第1のライセンスデータ暗号化処理部に対して出力する第3のライセンスデータ暗号化部をさらに含み、

前記コンテンツ再生部は、

前記第4の公開暗号鍵によって暗号化された前記再生情報を復号できる第4の秘密復号鍵を保持する第6の鍵保持部と、

前記第4の復号処理部の出力を受けて、前記第6の鍵保持部に保持された前記第4の秘密復号鍵によって前記再生情報(AC//Kc2)を復号し、前記ライセンスキー(Kc)を抽出して前記コンテンツデータ再生部(1516, 1518)に対して出力するための第6の復号処理部をさらに含む、請求の範囲第5項に記載のデータ配信システム。

9. 前記配信データ解読部(110, 210)は、前記端末(100, 101)に着脱可能な記録装置である、請求の範囲第1項に記載のデータ配信システム。

10. 前記記録装置は、メモリカードである、請求の範囲第9項に記載のデータ配信システム。

11. 前記第1のインターフェース部(350)と前記第2のインターフェース部(1202)とは、携帯電話網によって接続される、請求の範囲第1項に記載のデータ配信システム。

12. 前記記憶部(1415, 1430, 1440)は、外部から直接アクセス不可能なセキュリティ領域(TRM)内に配置される、請求の範囲第1項に記載のデータ配信システム。

13. 前記記憶部(1415, 1430, 1440)は、
前記暗号化コンテンツデータを記録するための第1の記憶ブロック(1415)と、

前記アクセス制限情報を記録するための第2の記憶ブロック(1440)とを含み、

前記第1の記憶ブロックは、前記再生情報を暗号化された状態でさらに記録し、
前記第2の記憶ブロックは、外部から直接アクセス不可能なセキュリティ領域(TRM)内に配置される、請求の範囲第1項に記載のデータ配信システム。

14. 前記記憶部(1415, 1430, 1440)は、
前記暗号化コンテンツデータを記録するための第1の記憶ブロック(1415)と、

前記アクセス制限情報および前記再生情報を記録するための第2の記憶ブロック（1430, 1440）とを含み、

前記第2の記憶ブロックは、外部から直接アクセス不可能なセキュリティ領域（TRM）内に配置される、請求の範囲第1項に記載のデータ配信システム。

5 15. 前記配信制御部（315）は、配信先の前記配信データ解読部（110, 120）を認証した後に、前記再生情報（Kc//AC2, {Kc//AC2} Kcom）と前記アクセス制限情報（AC1）とを前記第1のインターフェース部（350）を介して出力する、請求の範囲第1項に記載のデータ配信システム。

10 16. 前記配信データ解読部（110, 120）は、外部から前記再生情報（Kc//AC2, {Kc//AC2} Kcom）の出力が指示された場合に、出力先を認証した後に、前記再生情報を前記第2のインターフェース部（1102）を介して出力する、請求の範囲第1項に記載のデータ配信システム。

15 17. 前記制御部（1420）は、前記複製動作において、他の配信データ解読部（112）に対しての前記アクセス制限情報（AC1）を前記再生情報（Kc//AC2, {Kc//AC2} Kcom）とともに出力し、

前記制御部は、前記他の配信データ解読部に対する前記複製制限情報（Sub_Move）を生成するとともに、前記記憶部（1415, 1430, 1430）に記録された前記アクセス制限情報に含まれる前記複製制限情報を、生成した前記複製制限情報に変更した前記アクセス制限情報を前記他の配信データ解読部に対して出力する、請求の範囲第3項に記載のデータ配信システム。

18. 前記制御部（1420）は、前記複製動作において、他の配信データ解読部（112）に対しての前記アクセス制限情報（AC1）を前記再生情報（Kc//AC2, {Kc//AC2} Kcom）とともに出力し、

前記制御部は、前記他の配信データ解読部に対する前記複製制限情報（Sub_Move）を生成するとともに、前記記憶部（1415, 1430, 1430）に記録された前記アクセス制限情報に含まれる前記複製制限情報を、生成した前記複製制限情報に変更し、

前記第4の暗号化処理部は、変更した前記アクセス制限情報を暗号化して、前記再生情報とともに前記第1の暗号化処理部へ与える、請求の範囲第6項に記載

のデータ配信システム。

19. 記録装置であって、

外部との間でデータを授受するためのインターフェース部（1202）と、

前記インターフェース部を介して入力される、格納データ（Kc//AC2, {Kc//AC2}

5 Kcom）および前記格納データの前記記録装置からの出力を制御するためのアクセス制限情報（AC1）を記録するための記憶部（1415, 1430, 1440）と、

外部から前記格納データの出力が指示された場合に、前記記憶部に記録された前記アクセス制限情報に基づいて前記出力の可否を判断する制御部（1420）とを備える、記録装置。

10 20. 前記アクセス制限情報（AC1）は、前記記録装置から他の機器（100, 101）への前記格納データ（Kc//AC2, {Kc//AC2} Kcom）の出力回数を制限する出力回数制御情報（Sub_Play）を含み、

15 前記制御部（1420）は、前記他の機器に対する前記格納データの出力が指示された場合において、前記出力回数制御情報に基づいて前記出力の可否を判断するとともに、前記出力後、必要に応じて前記出力回数制御情報を更新可能である、請求の範囲第19項に記載の記録装置。

20 21. 前記アクセス制限情報（AC1）は、他の前記記録装置（112）に対する前記格納データ（Kc//AC2, {Kc//AC2} Kcom）の複製可能回数を制限する複製制限情報（Sub_Move）を含み、

前記制御部（1420）は、前記他の記録装置に対する前記格納データの複製指示が外部から指示された場合において、前記複製制限情報に基づいて前記格納データの出力の可否を判断するとともに、前記出力後、必要に応じて前記複製制限情報を更新可能である、請求の範囲第19項に記載の記録装置。

25 22. 前記記憶部は、前記アクセス制限情報（AC1）を記録するための記憶ブロック（1440）を有し、

前記記録装置は、

前記記録装置に対応して予め定められる公開暗号鍵（KPm(i)）によって暗号化されたデータを復号するための秘密復号鍵（Km(i)）を保持する秘密鍵保持部

(1421) と、

前記インターフェース部(1202)を介して入力される、前記公開暗号鍵によって暗号化された前記アクセス制限情報(AC1)を復号して、前記記憶ブロックに与えるアクセス制限情報復号部(1422)とをさらに備える、請求の範囲第5 19項に記載の記録装置。

23. 前記記憶ブロック(1430, 1440)は、外部から直接アクセス不可能なセキュリティ領域(TRM)内に配置される、請求の範囲第22項に記載の記録装置。

24. 認証鍵(KPma)によって復号可能な状態に暗号化された、前記記録装置10 に対応して定められる第1の公開暗号鍵(KPmc(m))を保持し、前記格納データ(Kc//AC2, {Kc//AC2} Kcom)および前記アクセス制限情報(AC1)を受信する場合において前記インターフェース部(1202)を介して外部に出力する認証データ保持部(1400)と、

前記第1の公開暗号鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵(Kmc(m))を保持する第1の鍵保持部(1442)と、

前記第1の公開暗号鍵によって暗号化された第1の共通鍵(Ks1)を前記インターフェース部を介して外部から受けて、復号処理するための第1の復号処理(1404)と、

前記記録装置ごとに異なる第2の公開暗号鍵(KPm(i))を保持する第2の鍵保持部(1416)と、

前記格納データの通信ごとに更新される第2の共通鍵(Ks2)を生成するセッションキー発生部(1418)と、

前記第2の共通鍵および前記第2の公開暗号鍵を前記第1の共通鍵によって暗号化し、前記インターフェース部を介して外部に出力するための第1の暗号化処理部(1406)と、

前記インターフェース部を介して、前記第2の共通鍵および前記第2の公開暗号鍵によって暗号化されて入力される前記格納データおよび前記アクセス制限情報を受けて、前記第2の共通鍵によって復号するための第2の復号処理部(1412)と、

前記第2の公開暗号鍵によって暗号化されたデータを復号するための第2の秘密復号鍵 ($K_m(i)$) を保持する第3の鍵保持部 (1421) と、

暗号化された、前記格納データおよび前記アクセス制限情報を、前記第2の秘密復号鍵によって復号するための第3の復号処理部 (1422) とをさらに備え、

5 前記記憶部 (1415, 1430, 1440) は、前記格納データを、前記第2の公開暗号鍵によって暗号化された状態および、前記第3の復号処理部によって復号された状態のいずれか一方の状態で記録する、請求の範囲第19項に記載の記録装置。

10 25. 前記セッションキー発生部 (1418) は、外部から指示される、他の機器 (100, 101) への前記格納データ ($K_c//AC2$, $\{K_c//AC2\} K_{com}$) の出力指示である第1の出力指示に応じて、第3の共通鍵 (K_s3) を生成し、

前記記録装置は、

15 前記認証鍵 (K_{Pma}) によって復号可能な状態に暗号化された、前記他の機器に 対応して予め定められる第3の公開暗号鍵 ($K_{Pp}(n)$) を前記インターフェース部 (1202) を介して受けて、前記認証鍵によって復号処理するための認証処理部 (1408) と、

前記第1の出力指示に応じて、前記認証処理部から受ける前記第3の公開暗号鍵によって前記第3の共通鍵を暗号化して、前記他の機器に対して出力する第2の暗号化処理部 (1410) とをさらに備え、

20 前記インターフェース部は、前記第1の出力指示に応じて、前記第3の共通鍵によって暗号化されて返信される、前記他の機器において生成された第4の共通鍵 (K_{s4}) を受けて前記第2の復号処理部 (1412) に伝達し、

前記第2の復号処理部は、前記第1の出力指示に応じて、前記セッションキー発生部から受けた前記第3の共通鍵によって、前記第3の共通鍵によって暗号化された前記第4の共通鍵を抽出し、

前記記憶部は、前記制御部 (1420) に制御されて、前記第1の出力指示に応じて、前記格納データを出力し、

前記第3の復号処理部 (1422) は、前記第1の出力指示に応じて、前記記憶部から出力された前記格納データが暗号化されている場合に、復号を行なって

前記格納データを抽出し、

前記第2の復号処理部(1412)は、前記第1の出力指示に応じて、前記第3の共通鍵によって暗号化されて前記端末から返信されるデータを復号して、前記再生動作を行なう前記端末において前記格納データの通信ごとに更新される第5 4の共通鍵(Ks4)を抽出し、

前記第1の暗号化処理部(1406)は、前記第1の出力指示に応じて、前記第3の復号処理部および前記記憶部のいずれか一方から前記格納データを受けて、前記第2の復号処理部(1412)で抽出された前記第4の共通鍵によって暗号化して、前記インターフェース部を介して前記他の機器に出力し、

10 前記アクセス制限情報(AC1)は、前記記録装置から他の機器への前記格納データの出力回数を制限する出力回数制御情報(Sub_Play)を含み、

前記制御部(1420)は、前記第1の出力指示に応じて前記記録装置内の各部の動作を制御し、前記出力回数制御情報に基づいて前記格納データの出力の可否を判断し、前記格納データの出力後、必要に応じて前記出力回数制御情報を更新する、請求の範囲第24項に記載の記録装置。

15 26. 前記セッションキー発生部(1418)は、外部から指示される、前記記録装置から他の記録装置(112)への前記格納データ(Kc//AC2, {Kc//AC2}Kcom)の出力指示である第2の出力指示に応じて、前記第3の共通鍵(Ks3)を生成し、

20 前記認証処理部(1408)は、前記第2の出力指示に応じて、前記他の記録装置に対応する前記第1の公開暗号鍵(KPmc(m))を復号処理によって取得し、

前記第2の暗号化処理部(1410)は、前記第2の出力指示に応じて、前記他の記録装置に対応する前記第1の公開暗号鍵によって、前記記録装置に対応する前記第3の共通鍵を暗号化して前記他の記録装置に対して出力し、

25 前記第2の復号処理部(1412)は、前記第2の出力指示に応じて、前記記録装置に対応する前記第3の共通鍵で暗号化されて前記他の記録装置から返信されるデータを復号して、前記他の記録装置で生成された前記第2の共通鍵(Ks2)および前記他の記録装置に対応する前記第2の公開暗号鍵(KPm(i))を取得し、

前記記憶部は、前記制御部（1420）に制御されて、前記第2の出力指示に応じて、前記格納データを出力し、

- 前記第3の復号処理部（1422）は、前記第2の出力指示に応じて、前記記憶部から出力された前記格納データが暗号化されている場合に、復号を行なって
5 前記格納データを抽出し、

前記記録装置は、

- 前記第2の出力指示がなされた場合において、前記第3の復号処理部および前記記憶部のいずれか一方から受けた前記格納データを、前記他の記録装置に対応する前記第2の公開暗号鍵によって暗号化するための第3の暗号化処理部（14
10 24）をさらに有し、

- 前記第1の暗号化処理部（1406）は、前記第2の出力指示に応じて、前記第3の暗号化処理部の出力を、前記他の記録装置で生成された前記第2の共通鍵によってさらに暗号化して、前記インターフェース部を介して前記他の記録装置に出力し、
15 前記アクセス制限情報（AC1）は、前記他の記録装置に対する前記格納データの出力可能回数を制限する複製制限情報を含み、

- 前記制御部（1420）は、前記第2の出力指示に応じて前記記録装置内の各部の動作を制御し、前記複製制限情報に基づいて前記第2の出力指示の実行の可否を判断し、前記第2の出力指示の実行後において、必要に応じて前記複製制限
20 情報を更新する、請求の範囲第25項に記載の記録装置。

27. 前記記憶部（1415, 1430, 1440）は、前記インターフェース部（1202）を介して外部から入力される暗号化コンテンツデータ（{Data}
Kc）をさらに記録し、

- 前記格納データ（Kc//AC2, {Kc//AC2} Kcom）は、前記暗号化コンテンツデータを復号して平文のコンテンツデータ（Data）を得るための復号鍵であるライセンスキー（Kc）を含む、請求の範囲第19項に記載の記録装置。
25

28. 前記記録装置は、メモリカードである、請求の範囲第19項に記載の記
録装置。

29. 前記記憶部（1415, 1430, 1440）は、外部から直接アクセ

ス不可能なセキュリティ領域 (TRM) 内に配置される、請求の範囲第 19 に記載の記録装置。

30. 記憶部 (1415, 1430, 1440) は、

外部から直接アクセス不可能なセキュリティ領域 (TRM) 内に配置される第 5 1 の記憶ブロック (1430, 1440) と、

外部から直接アクセス可能な第 2 の記憶ブロック (1415) とを含み、

前記アクセス制限情報(AC1)は、前記第 1 の記憶ブロックに記録され、

前記格納データ (Kc//AC2, {Kc//AC2} Kcom) は、暗号化されて前記第 2 の記憶ブロックに記録される、請求の範囲第 19 項に記載の記録装置。

10 31. 記憶部 (1415, 1430, 1440) は、

外部から直接アクセス不可能なセキュリティ領域 (TRM) 内に配置される第 1 の記憶ブロック (1430, 1440) と、

外部から直接アクセス可能な第 2 の記憶ブロック (1415) とを含み、

前記格納データ (Kc//AC2, {Kc//AC2} Kcom) およびアクセス制限情報(AC1)は、

15 前記第 1 の記憶ブロックに記録される、請求の範囲第 19 項に記載の記録装置。

32. 前記制御部 (1420) は、前記格納データ (Kc//AC2, {Kc//AC2} Kcom) の出力を指示された場合に、出力先を認証した後に、前記格納データを出力する、請求の範囲第 19 項に記載の記録装置。

33. 前記制御部 (1420) は、他の記録装置 (112) に対しての前記アクセス制限情報(AC1)を前記格納データ (Kc//AC2, {Kc//AC2} Kcom) とともに出力し、

前記制御部は、前記他の記録装置に対する前記複製制限情報 (Sub_Move) を生成するとともに、前記記憶部 (1415, 1430, 1430) に記録された前記アクセス制限情報に含まれる前記複製制限情報を、生成した前記複製制限情報 25 に変更した前記アクセス制限情報を前記他の記録装置に対して出力する、請求の範囲第 21 項に記載の記録装置。

34. 前記制御部 (1420) は、前記第 2 の出力指示において、他の記録装置 (112) に対しての前記アクセス制限情報(AC1)を前記格納データ (Kc//AC2, {Kc//AC2} Kcom) とともに出力し、

- 前記制御部は、前記他の記録装置に対する前記複製制限情報（Sub_Move）を生成するとともに、前記記憶部（1415, 1430, 1430）に記録された前記アクセス制限情報に含まれる前記複製制限情報を、生成した前記複製制限情報に変更し、
- 5 前記第3の暗号化処理部は、前記格納データとともに、変更した前記アクセス制限情報を暗号化し、前記第1の暗号化処理部へ与える、請求の範囲第26項に記載の記録装置。

FIG. 1

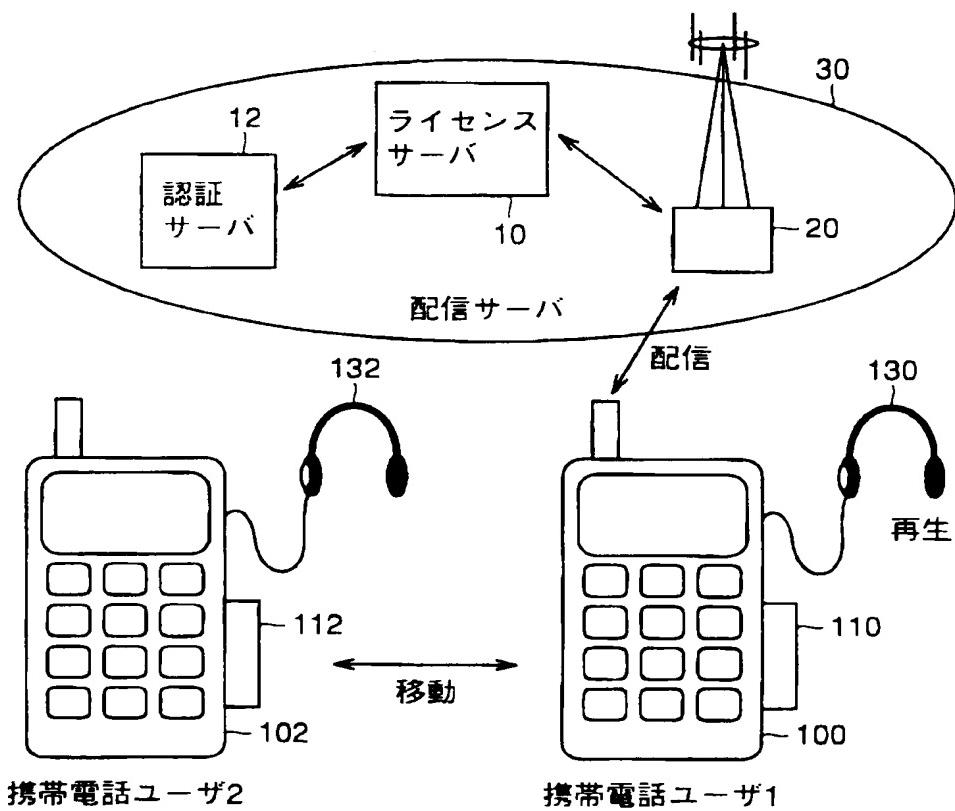


FIG.2

| 名称 | 属性 | 保持／発生箇所 | 機能・特徴 |
|----------|-------------|---------|--|
| Data | コンテンツデータ | | 例：音楽データ |
| Kc | ライセンスキー | | 暗号化コンテンツデータの復号鍵 |
| {Data}Kc | 暗号化コンテンツデータ | | 共通鍵KCで復号可能な暗号化が施されたコンテンツデータ この形式で配信サーバにより配布。 |
| Data-inf | 附加情報 | | 例：コンテンツデータに関する著作権あるいは サーバアクセス関連等の平文情報 |
| コンテンツID | コンテンツに関する情報 | 配信サーバ | コンテンツデータDataを識別するコード |
| ライセンスID | ライセンスに関する情報 | | ライセンスの発行を特定できる管理コード (コンテンツIDを含めて識別することも可) |
| AC | ライセンス購入条件 | | 利用者側から指定(例：ライセンス数、機能限定等) メモリのアクセスに対する制限(例：再生可能回数) |
| AC1 | アクセス制限情報 | | コンテンツ再生回路(携帯電話機)における制御情報 |
| AC2 | 再生回路制御情報 | | (例：再生可否) |

| 名称 | 属性 | 保持／発生箇所 | 機能・特徴 |
|---------|------------------|---|--|
| KPp(n) | 公開暗号化鍵 (非対称鍵) | 携帯電話機 | Kp(n)にて復号可能。 (KP(n)//Cp(n)) KPmaの形式で出荷時に記録 nは携帯電話機の種類を区別する値。 |
| KPmc(m) | 公開暗号化鍵 (非対称鍵) | メモリカード | Kmc(i)にて復号可能。 (KPmc(m)//Cmc(m)) KPmaの形式で出荷時に記録 mはメモリカードの種類を区別する値。 |
| Kp(n) | 秘密復号鍵 | 携帯電話機 | コンテンツ再生回路(携帯電話機)固有の復号鍵 nは携帯電話機の種類を区別する値。 |
| Kmc(m) | 秘密復号鍵 | メモリカード | メモリカード固有の復号鍵 mはメモリカードの種類を区別する値。 |
| Cp(n) | 携帯電話機 | コンテンツ再生回路のクラス証明書。 (KP(n)//Cp(n)) KPmaの形式で出荷時に記録 nは携帯電話機の種類を区別する値。 | |
| Cmc(m) | クラス証明書 | メモリカード | メモリカードのクラス証明書。 (KPmc(m)//Cmc(m)) KPmaの形式で出荷時に記録 mはメモリカードの種類を区別する値。 |
| Ks1 | 配信サーバ | | 配信セッション毎に発生 |
| Ks2 | 共通鍵 (セッション固有) | メモリカード | 配信／移動(受)セッション毎に発生 |
| Ks3 | | メモリカード | 再生／移動(送)セッション毎に発生 |
| Ks4 | | 携帯電話機 | 再生セッション毎に発生 |
| Km(i) | 秘密復号鍵 | メモリカード | メモリカードごと(i)に固有の復号鍵 Kpm(i)で暗号化されたデータはKm(i)で復号可能 |
| KPm(i) | 公開暗号化鍵 (非対称鍵) | メモリカード | メモリカードごと(i)に固有の暗号化鍵 |
| KPma | 認証鍵 (公開復号鍵) | 配信サーバ | 配信システム全体で共通。 |
| Kcom | 秘密復号鍵 | 携帯電話機 配信サーバ | 再生回路共通の秘密鍵。Kc, AC2の暗号化および復号 に利用。 (共通鍵方式, 公開鍵方式のいずれであっても可) |

FIG.3

FIG.4

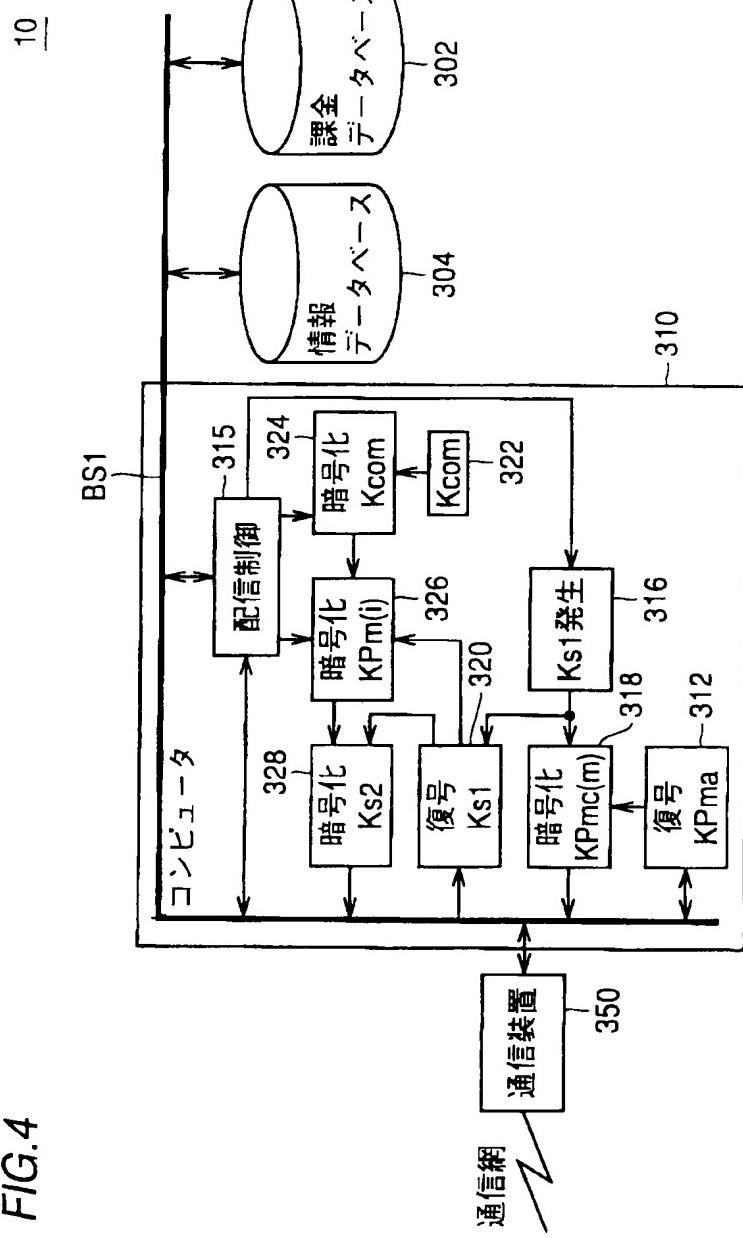


FIG.5

This block diagram illustrates a communication system architecture. The flow of signals is as follows:

- Antenna Input:** 1102 feeds into the **送受信** (Transceiver) block.
- Transceiver:** 1104 connects to the **切換** (Switching) block.
- Switching:** 1530 connects to the **音声再生** (Voice再生) and **音楽再生** (Music再生) blocks.
- Music/Music再生:** 1518 connects to the **切換** block.
- Switching:** 1525 connects to the **音声再生** and **音楽再生** blocks.
- Regeneration:** 1512 connects to the **音声再生** block.
- Modulation/Demodulation:** 1516 connects to the **音声再生** block.
- Demodulation:** 1506 connects to the **Ks4発生** (Ks4 Generation) block.
- Control:** $\{Kc/(AC2)\}Kcom$ connects to the **Ks4発生** block.
- Demodulation:** 1502 connects to the **Ks4復号** (Ks4 Demodulation) block.
- Demodulation:** 1500 connects to the **Kp(1)** block.
- Demodulation:** 1506 connects to the **Kp(1)** block.
- Demodulation:** 1502 connects to the **暗号化** (Encryption) block.
- Demodulation:** 1500 connects to the **暗号化** block.
- Demodulation:** 1504 connects to the **復号** (Decoding) block.
- Demodulation:** 1504 connects to the **Ks3** block.
- Demodulation:** 1504 connects to the **BS2** block.
- Demodulation:** 1510 connects to the **復号** block.
- Demodulation:** 1510 connects to the **Ks3** block.
- Demodulation:** 1510 connects to the **BS2** block.
- Demodulation:** 1514 connects to the **復号** block.
- Demodulation:** 1514 connects to the **Kc** block.
- Demodulation:** 1514 connects to the **BS2** block.
- Demodulation:** 1110 connects to the **コントローラ** (Controller) block.
- Demodulation:** 1110 connects to the **ディスプレイ** (Display) block.
- Demodulation:** 1110 connects to the **キー** (Key) block.
- Demodulation:** 1112 connects to the **音声再生** block.
- Demodulation:** 1112 connects to the **コントローラ** block.
- Demodulation:** 1112 connects to the **ディスプレイ** block.
- Demodulation:** 1112 connects to the **キー** block.
- Demodulation:** 1122 connects to the **外部インターフェース** (External Interface) block.
- Demodulation:** 1122 connects to the **メモリインターフェース** (Memory Interface) block.
- Demodulation:** 1122 connects to the **メモリカード** (Memory Card) block.
- Demodulation:** 1122 connects to the **コネクタ** (Connector) block.
- Demodulation:** 1122 connects to the **110** block.

FIG. 6

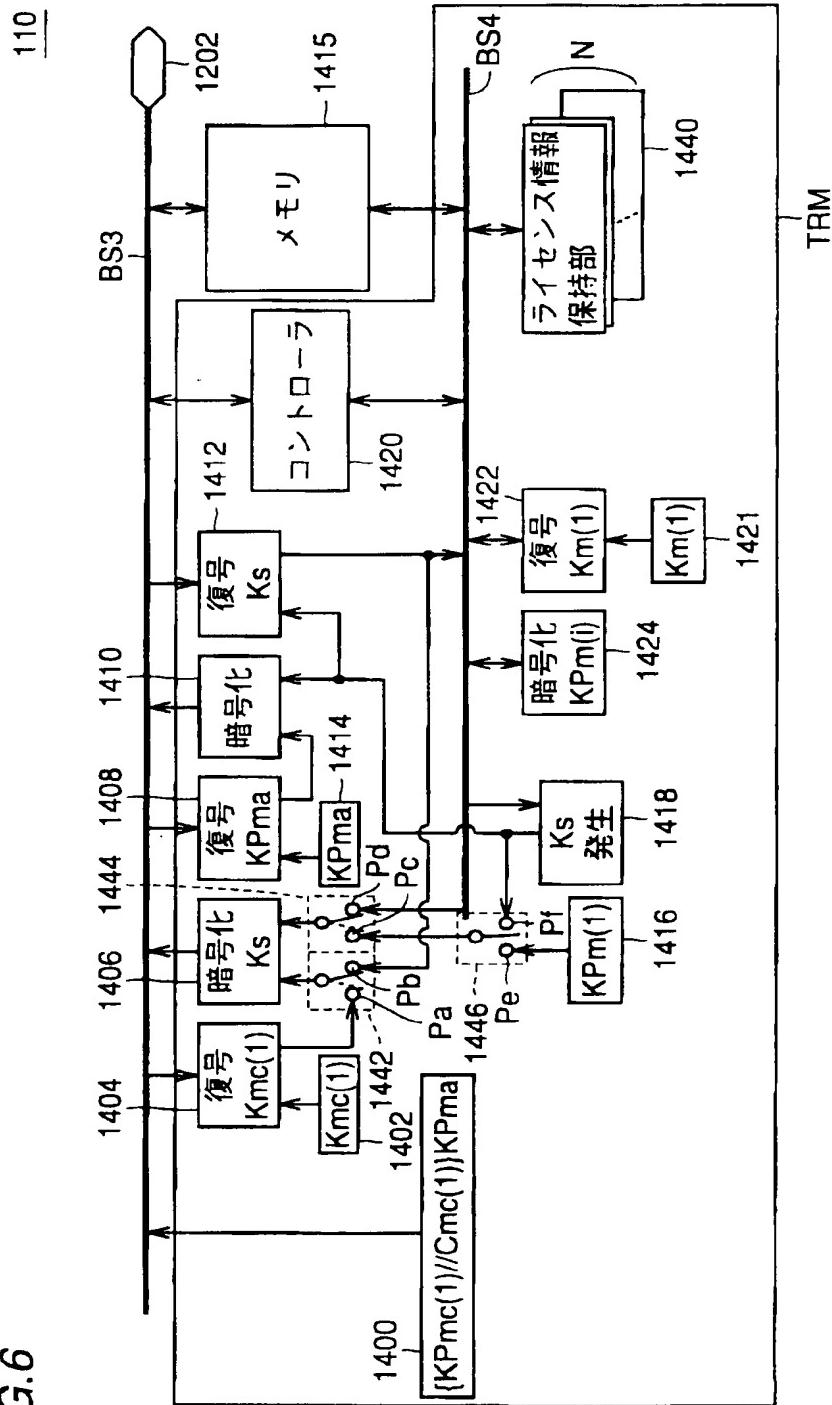


FIG.7

| | コンテンツID | ライセンスID | <u>Sub_Play</u> | <u>Sub_Move</u> |
|------|---------|---------|-----------------|-----------------|
| バンク1 | | | | |
| バンク2 | | | | |
| バンク3 | | | | |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| バンクN | | | | |

FIG.8

| | | |
|-----|----------|--------------------|
| AC1 | Sub_Play | 再生回数制限 |
| | | 0 : 再生不能 |
| | | 1~7F(h) : 再生可能回数 |
| | | 80~FE(h) : 未使用 |
| | Sub_Move | 所有ライセンス数 |
| | | 0 : ライセンス無 |
| | | 1~7F(h) : 所有ライセンス数 |
| | | 80~FE(h) : 未使用 |
| | | FF(h) : 移動禁止 |

FIG.9

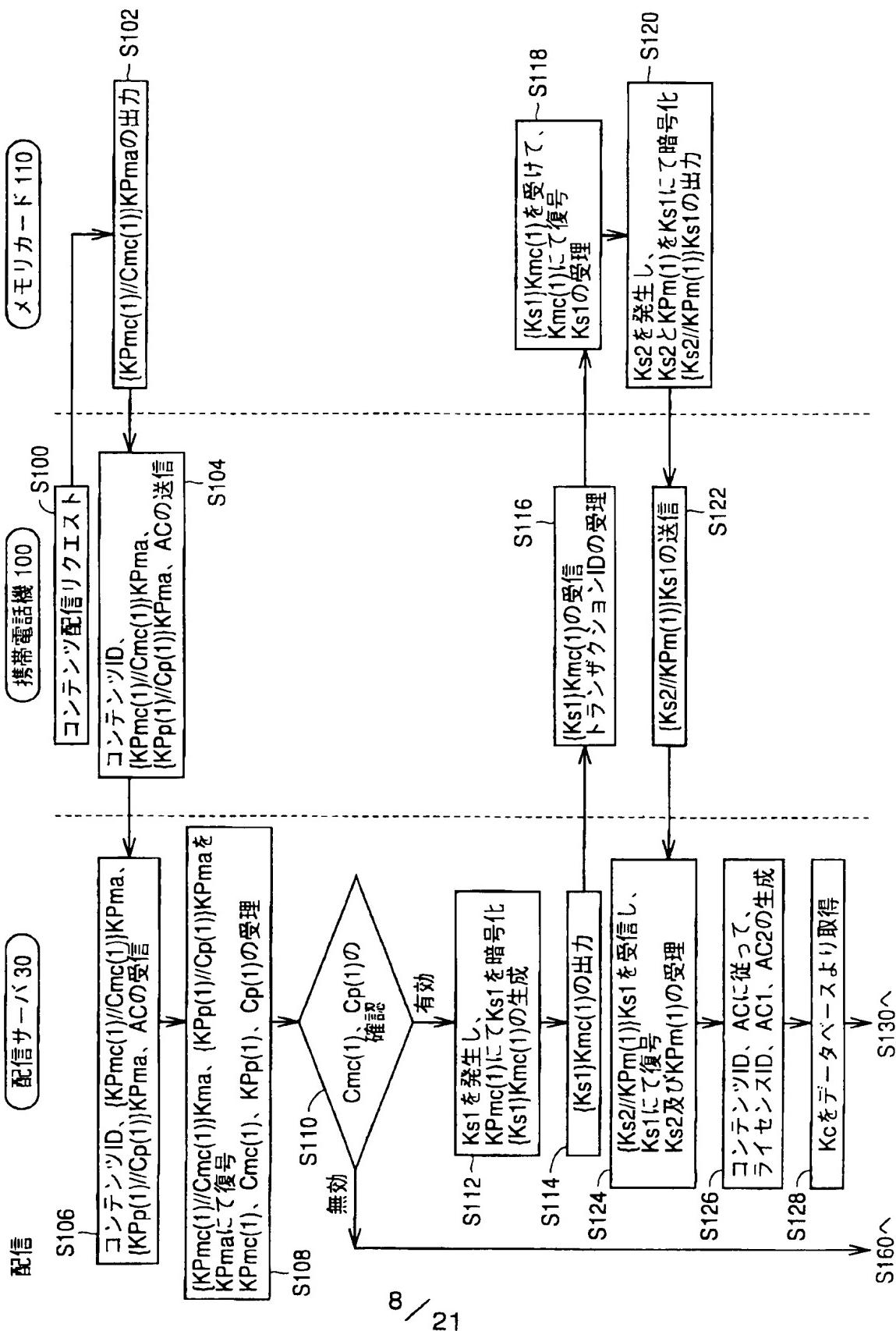


FIG. 10

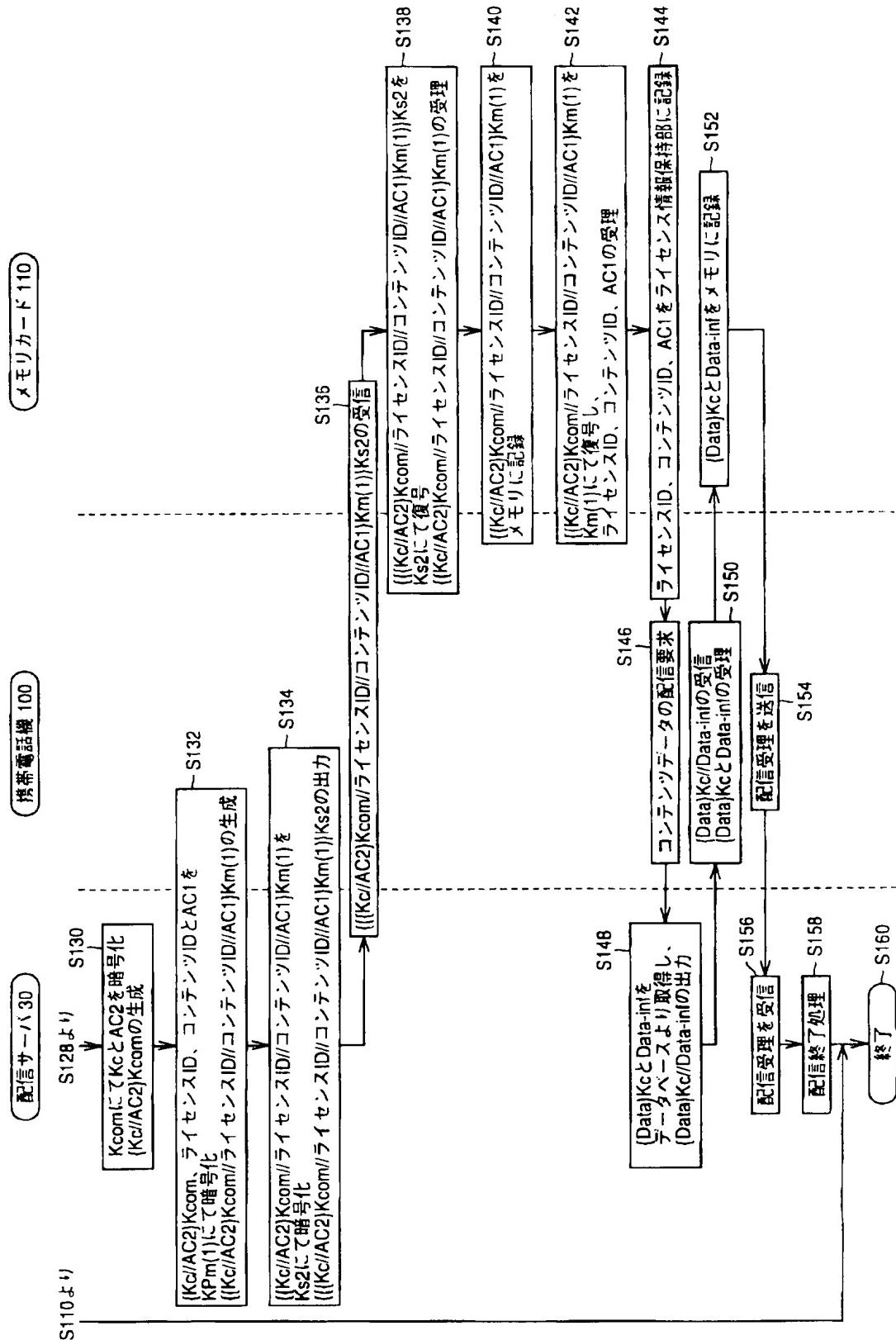


FIG. 11

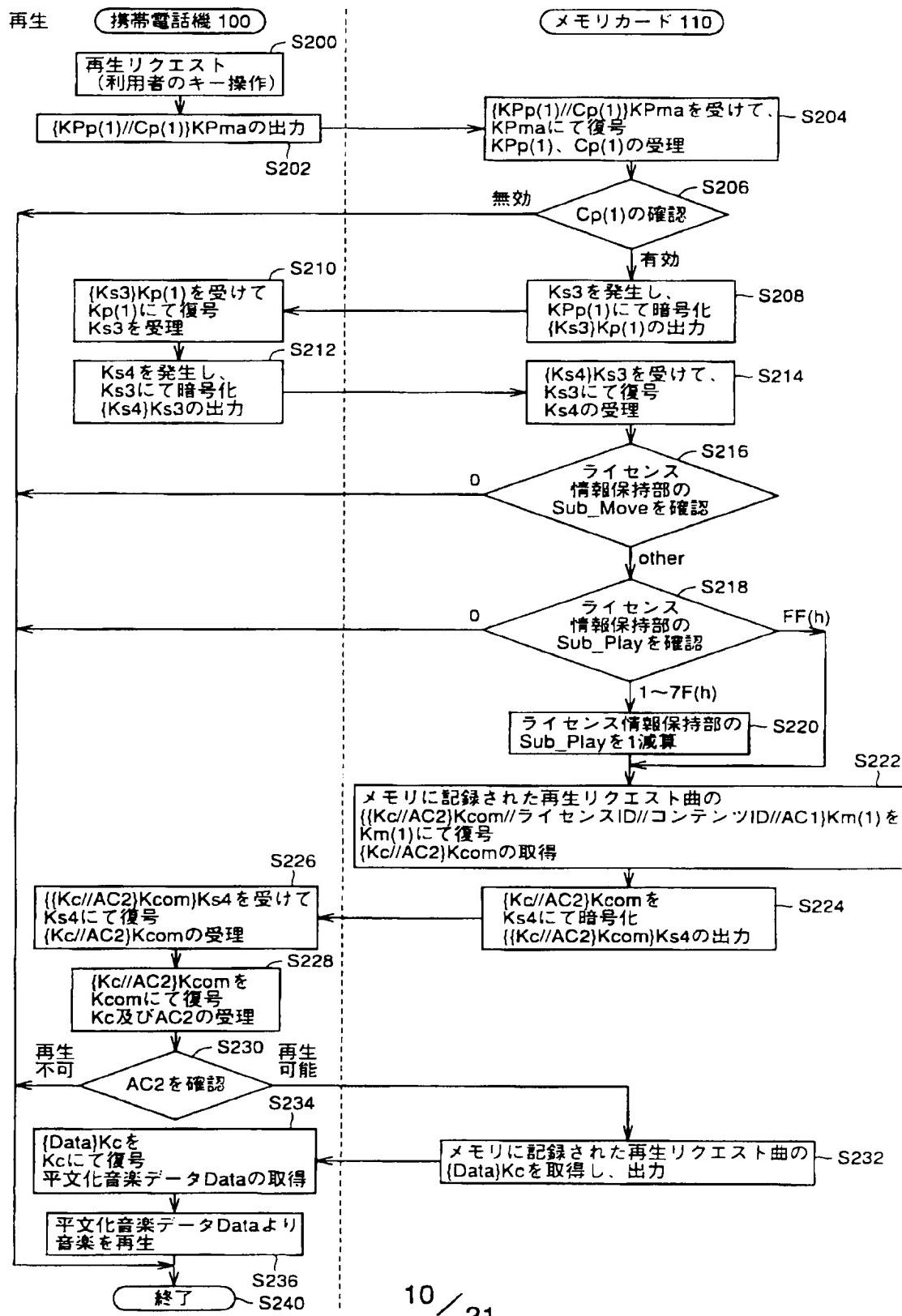


FIG.12

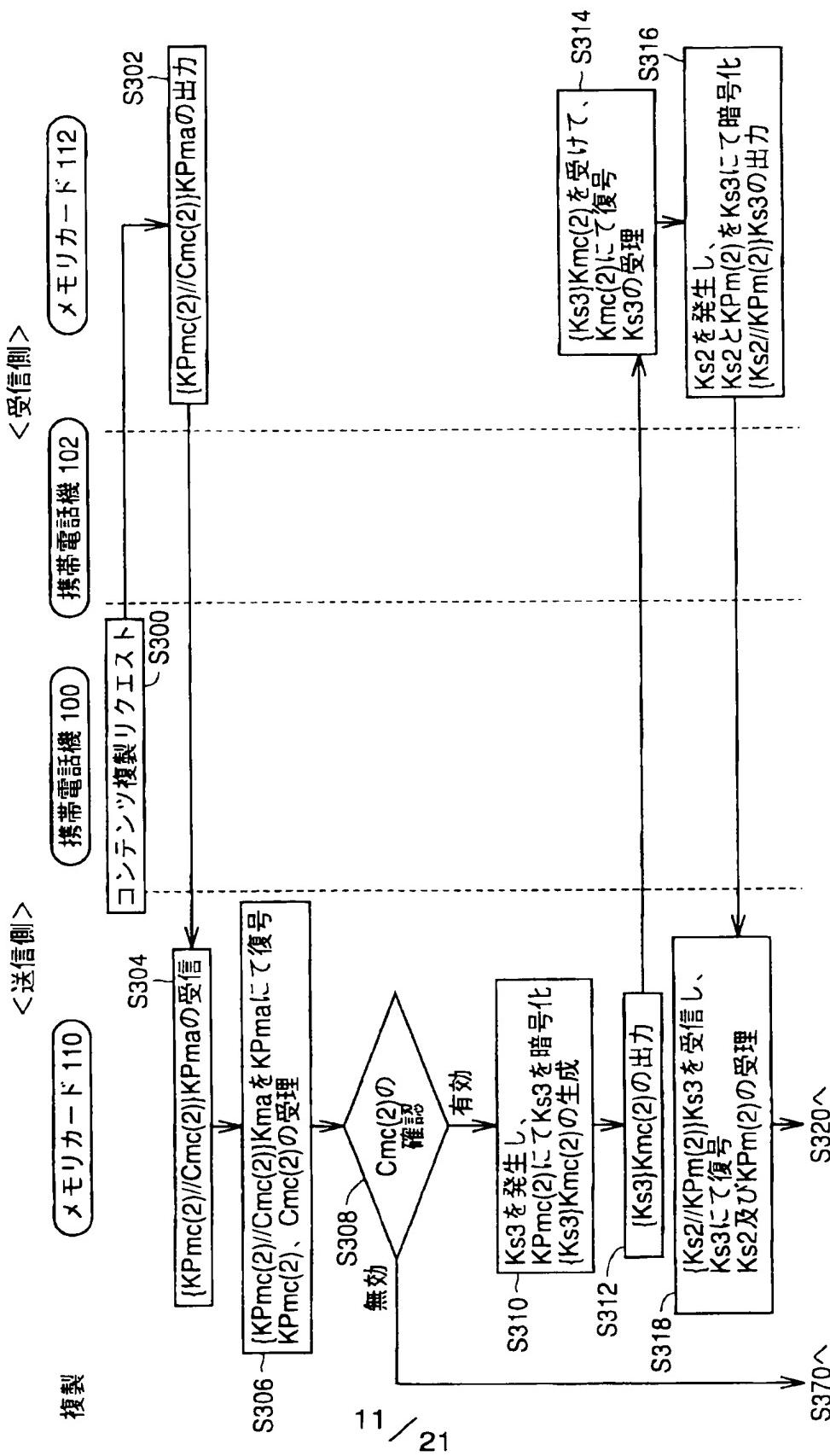


FIG. 13

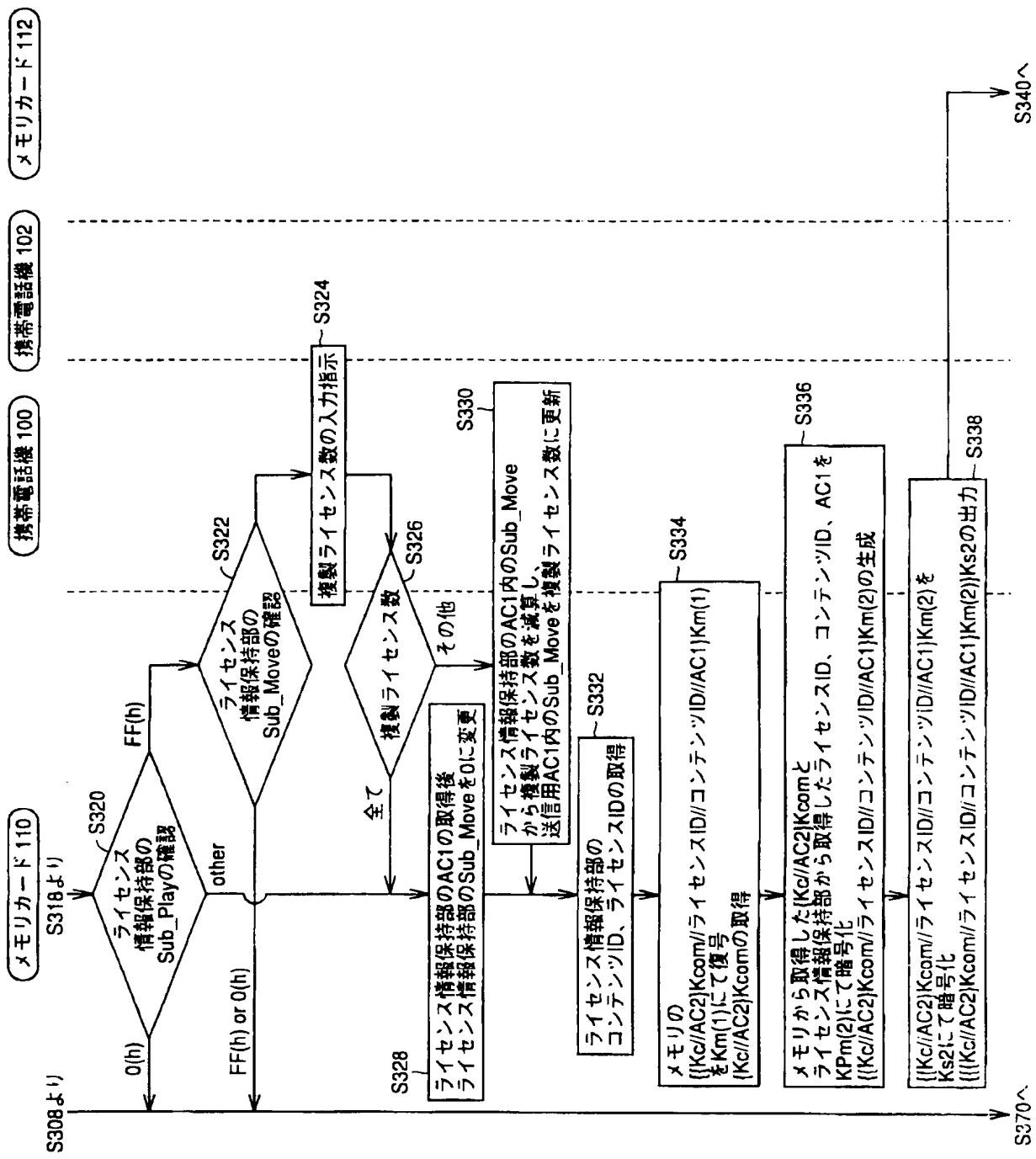
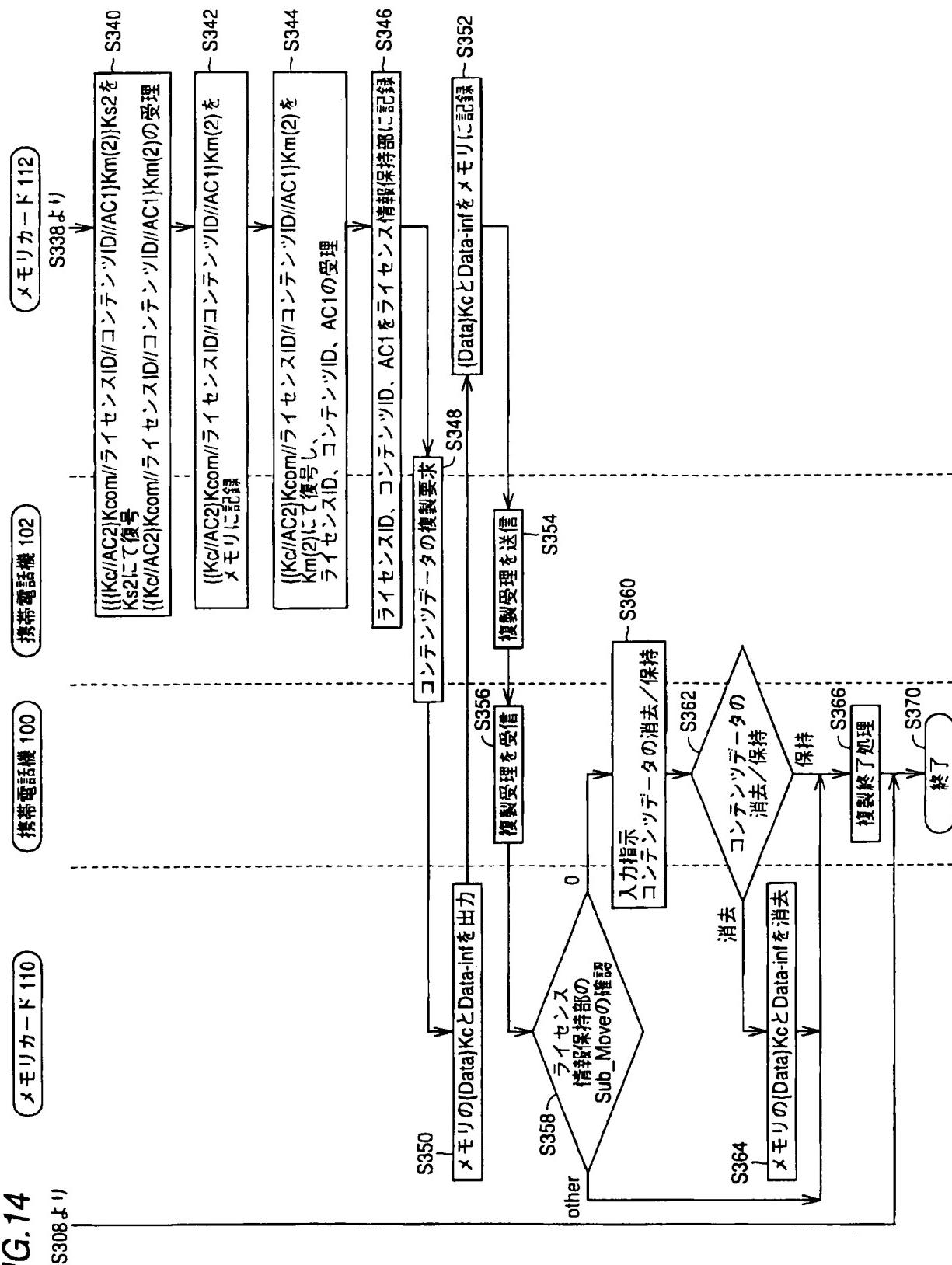


FIG. 14



11

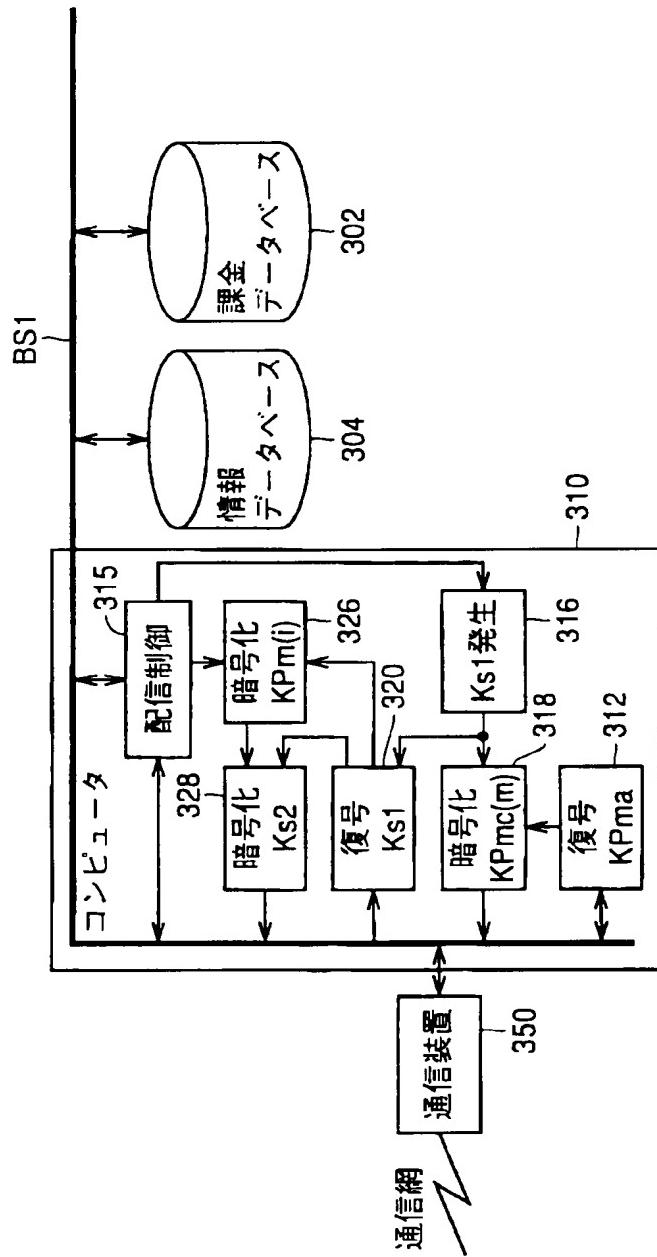


FIG. 15

FIG. 16

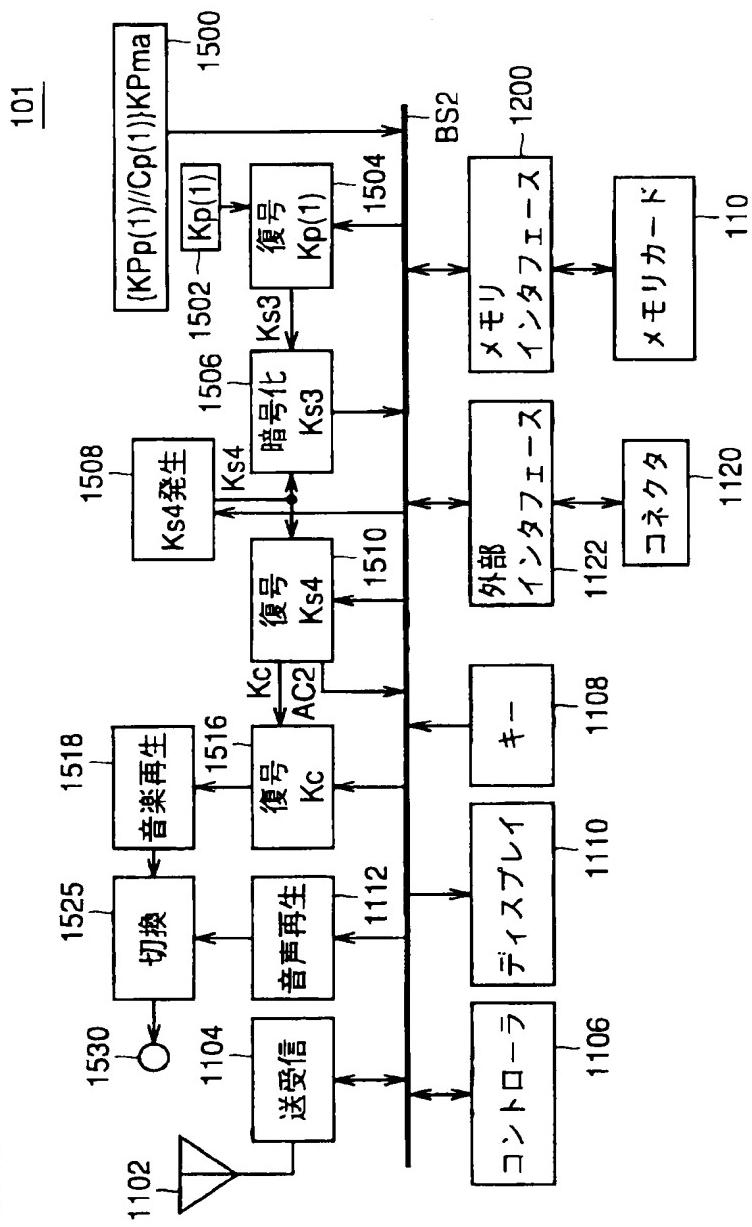


FIG. 17

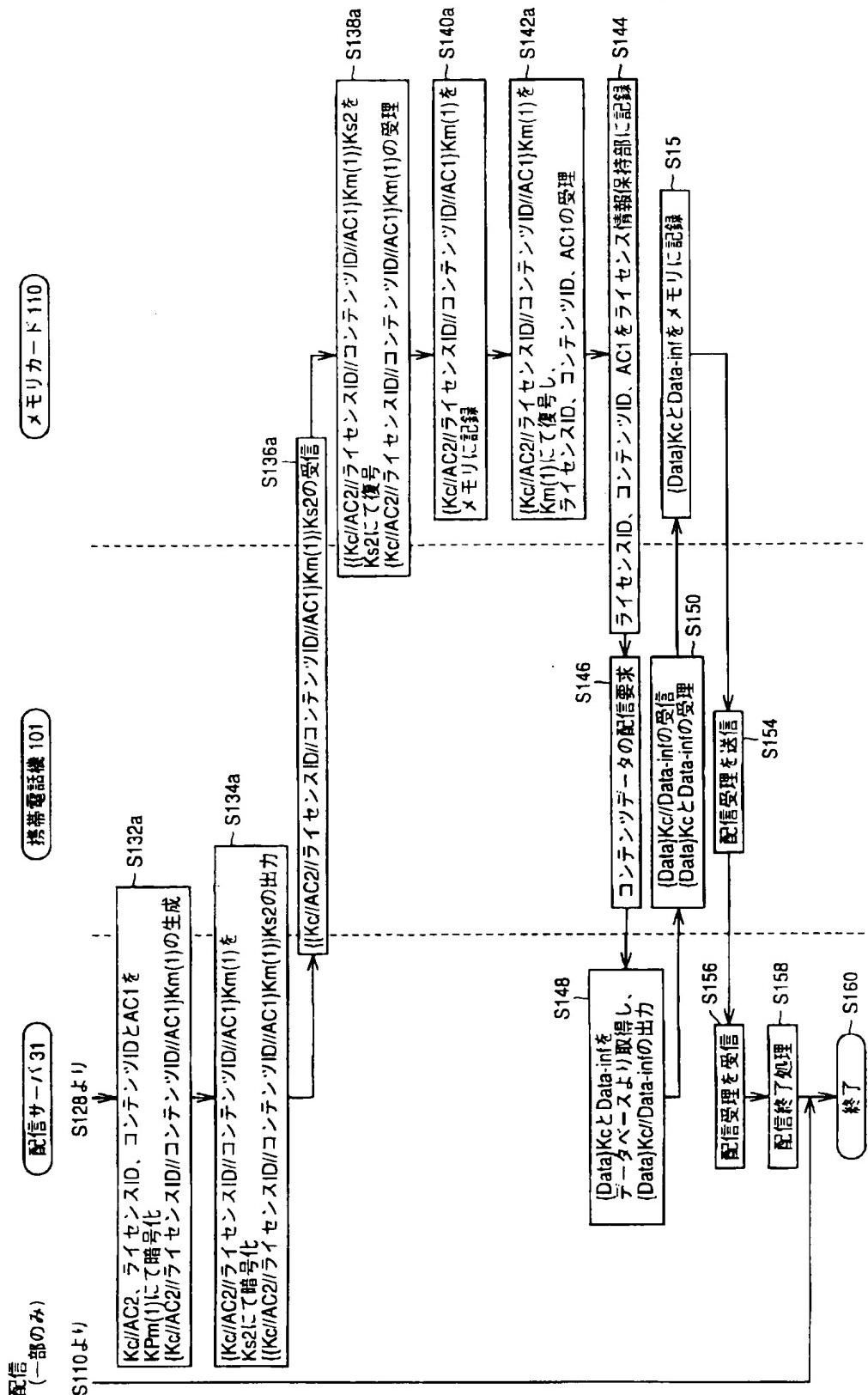


FIG. 18

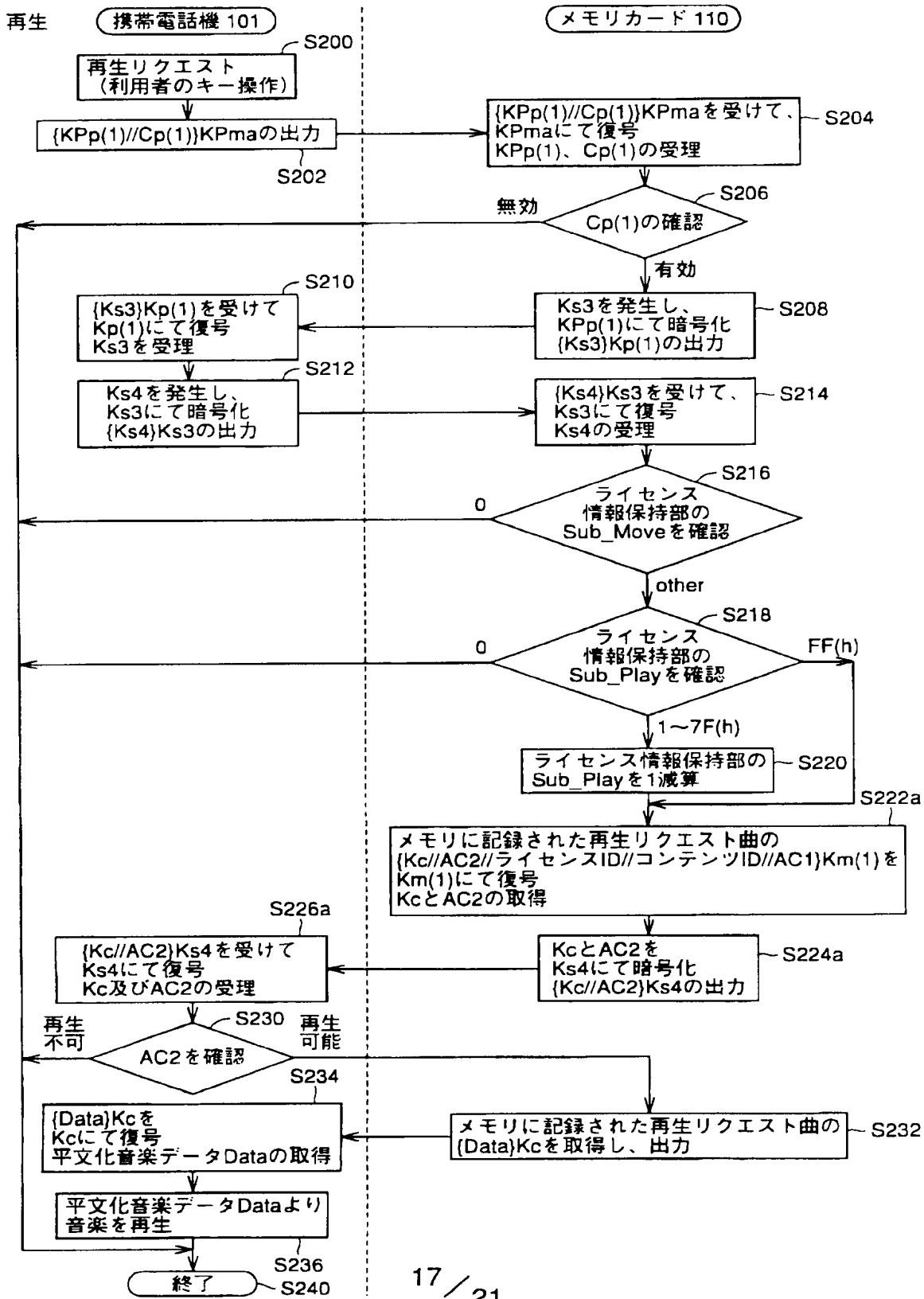


FIG. 19

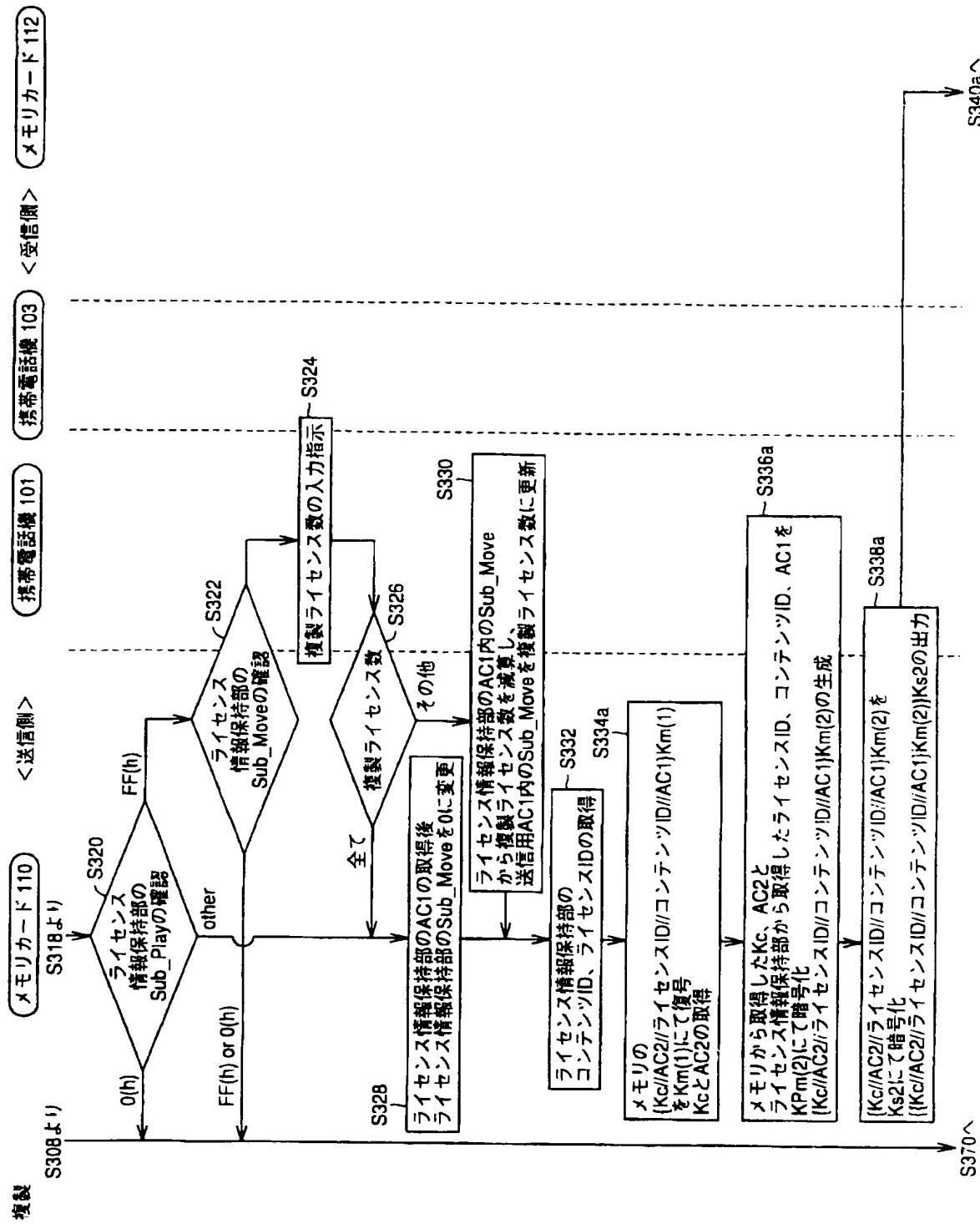


FIG.20

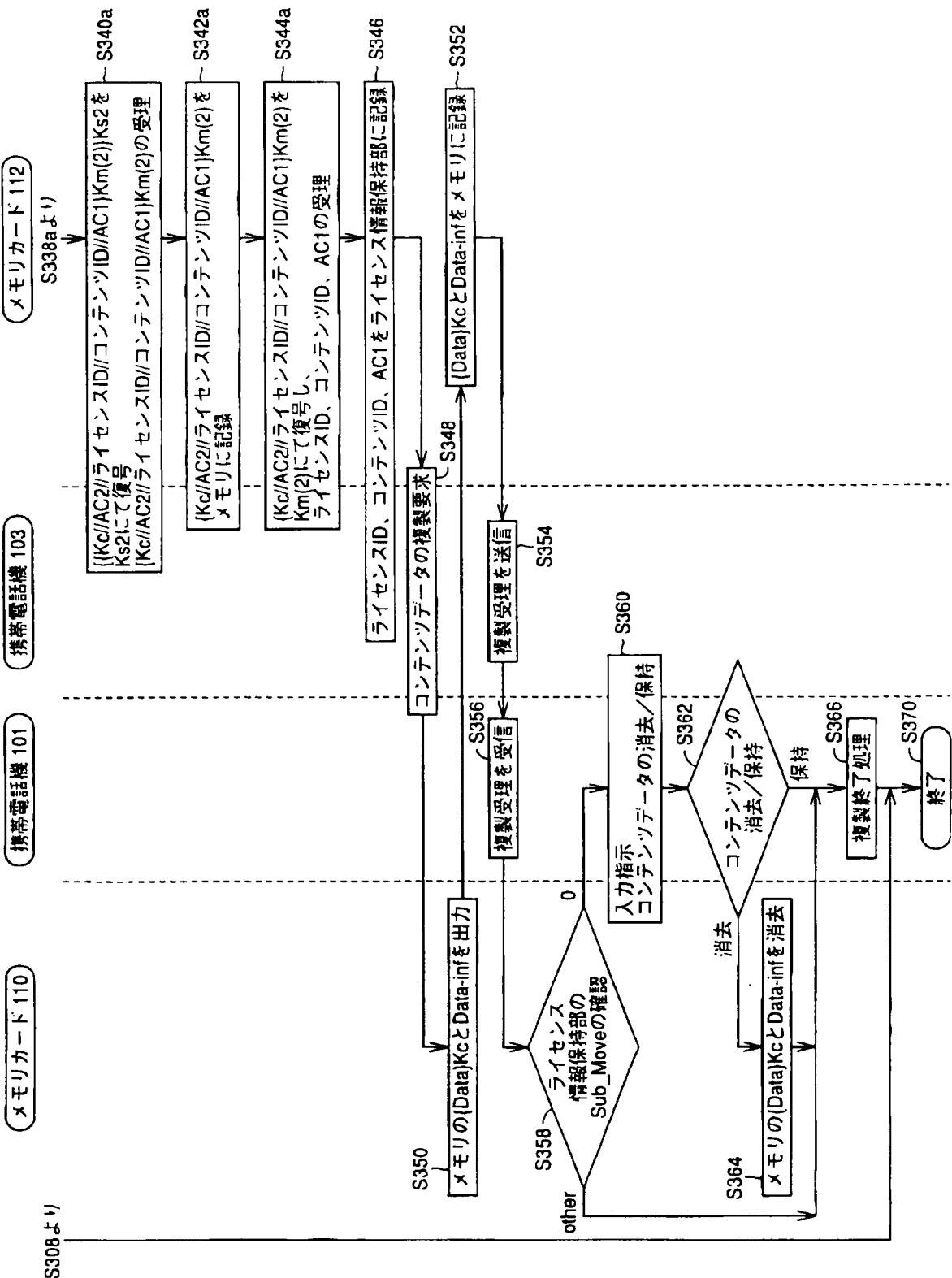
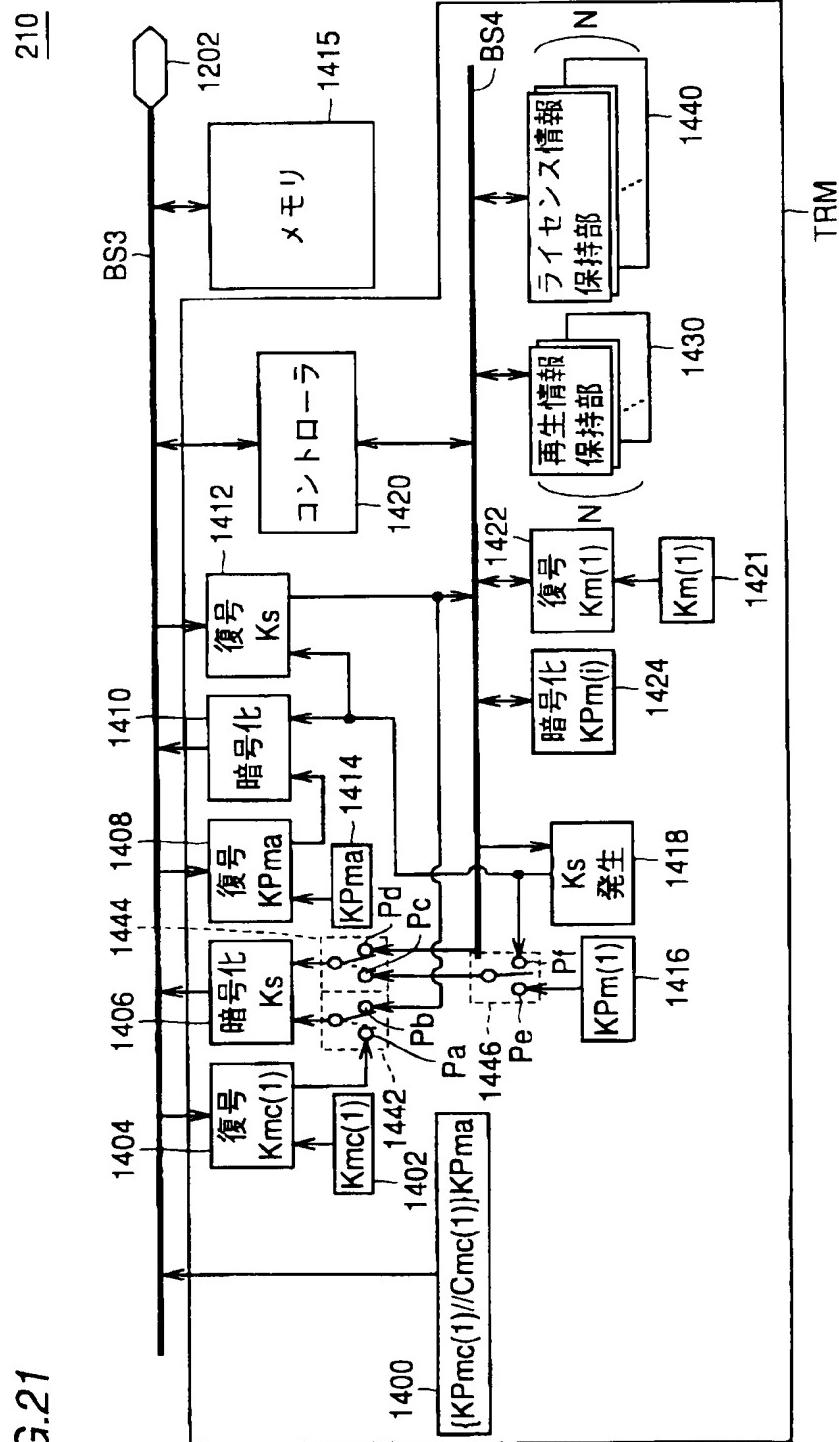
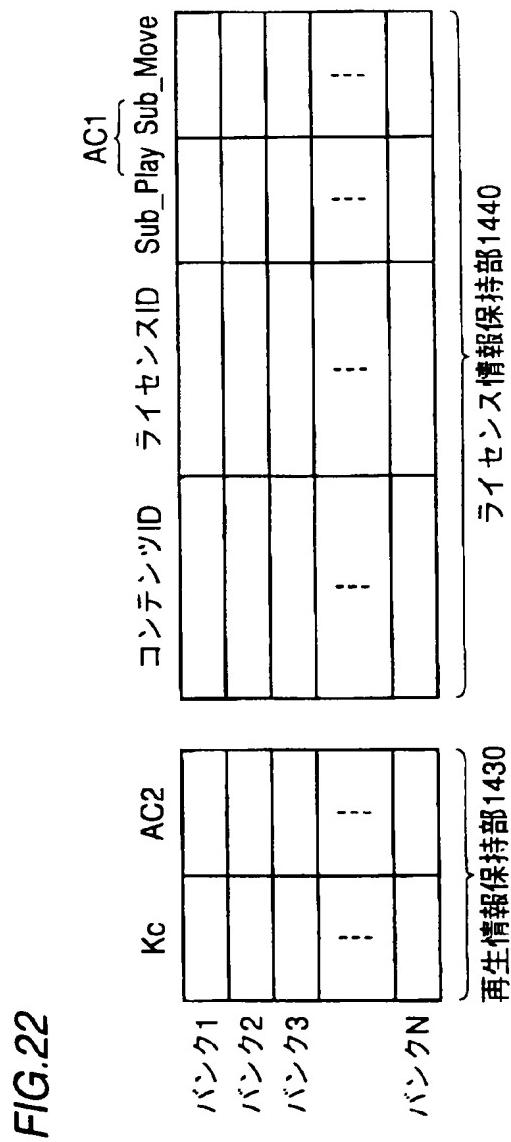


FIG.21





INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/08593

A. CLASSIFICATION OF SUBJECT MATTER
 Int.Cl⁷ H04L 9/32 G06F 12/14, 320 G10K 15/02 G06F 13/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
 Int.Cl⁷ H04L 9/00 H04K 1/00-3/00 G09C 1/00-5/00
 G06F 12/00-13/00 G10K 15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
 Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
 Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
 JICST FILE (JOIS)
 WPI (DIALOG)
 INSPEC (DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|-----------|---|----------------------------|
| Y | JP, 10-3745, A (Sony Corporation), 06 January, 1998 (06.01.98) & EP, 813194, A & CN, 1182268, A | 1-3, 9-17, 19-23, 27-33 |
| Y | Taro YOSHIO, "Kogata Memory Card de Ingaku Chosakuken wo mamoru", Nikkei Electronics, No. 739, (March, 1999), pp. 49-53 | 1-3, 9-17, 19-23, 27-33 |
| Y | Taro YOSHIO, "Jitsuyoki no Haishin System; Chosakuken Kanri ga Kagi wo nigiru", Nikkei Electronics, No. 738, (March, 1999), pp. 94-98 | 1-3, 9-17, 19-23, 27-33 |
| Y | JP, 11-164058, A (Hitachi Electron Service Co., Ltd.), 18 June, 1999 (18.06.99) (Family: none) | 11 |
| A | JP, 11-328850, A (Sony Corporation), 30 November, 1999 (30.11.99) & WO, 99/59092, A1 & EP, 996074, A | 1-34 |

Further documents are listed in the continuation of Box C.

See patent family annex.

| | |
|---|--|
| * Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed | "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family |
|---|--|

Date of the actual completion of the international search
 08 March, 2001 (08.03.01)

Date of mailing of the international search report
 21 March, 2001 (21.03.01)

Name and mailing address of the ISA/
 Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類(国際特許分類(IPC))

Int. C1⁷
H04L 9/32 G06F 12/14, 320 G10K 15/02 G06F 13/00

B. 調査を行った分野

調査を行った最小限資料(国際特許分類(IPC))

Int. C1⁷
H04L 9/00 H04K 1/00-3/00 G09C 1/00-5/00
G06F 12/00-13/00 G10K 15/00

最小限資料以外の資料で調査を行った分野に含まれるもの

| | |
|-------------|------------|
| 日本国実用新案公報 | 1922-1996年 |
| 日本国公開実用新案公報 | 1971-2001年 |
| 日本国登録実用新案公報 | 1994-2001年 |
| 日本国実用新案登録公報 | 1996-2001年 |

国際調査で使用した電子データベース(データベースの名称、調査に使用した用語)

JICSTファイル (JOIS)
WPI (DIALOG)
INSPEC (DIALOG)

C. 関連すると認められる文献

| 引用文献の カテゴリー* | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する 請求の範囲の番号 |
|-----------------|--|----------------------------|
| Y | JP, 10-3745, A (ソニー株式会社) 6. 1月. 1998 (06. 01. 98) & EP, 813194, A & CN, 1182268, A | 1-3, 9-17, 19-23, 27-33 |
| Y | 芳尾太郎 “小型メモリ・カードで音楽著作権を守る” 日経エレクトロニクス, No. 739, (1999年3月), pp. 49-53 | 1-3, 9-17, 19-23, 27-33 |
| Y | 芳尾太郎 “実用期の配信システム、著作権管理がカギ握る” 日経エレクトロニクス, No. 738, (1999年3月), pp. 94-98 | 1-3, 9-17, 19-23, 27-33 |

C欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献(理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

08. 03. 01

国際調査報告の発送日

21.03.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官(権限のある職員)

丸山 高政

5W 9570

電話番号 03-3581-1101 内線 3574

| C (続き) . 関連すると認められる文献 | | |
|-----------------------|---|------------------|
| 引用文献の カテゴリー* | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する 請求の範囲の番号 |
| Y | J P, 11-164058, A (日立電子サービス株式会社) 18. 6月. 1999 (18. 06. 99), (ファミリーなし) | 11 |
| A | J P, 11-328850, A (ソニー株式会社) 30. 11月. 1999 (30. 11. 99) & WO, 99/59092, A1 & EP, 996074, A | 1-34 |